Summer 2010

Energy-efficient task-scheduling and networking protocols for secure wireless networks

Sandeep Kolli

Department:

ENERGY-EFFICIENT TASK-SCHEDULING AND NETWORKING PROTOCOLS FOR SECURE WIRELESS NETWORKS

by

SANDEEP CHOWDARY KOLLI

A THESIS

Presented to the faculty of the Graduate School of the
MISSOURI UNIVERSITY OF SCIENCE AND TECHNOLOGY
In partial fulfillment of the requirements for the degree
MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

2010

Approved by:
Maciej Zawodniok, Advisor
Ann Miller
Yahong Rosa Zheng

PUBLICATION THESIS OPTION

This thesis consists of following articles that have been submitted for publication:

Pages 5-40 are intended for submission to the *IEEE/ACM Transactions on Networking*

Pages 41-74 are intended for submission to the *Journal of Parallel and Distributed Processing,Elsevier*

ABSTRACT

The performance of wireless networks is dependent on a number of factors including the available energy, energy-efficiency, data processing delay, transmission delay, routing decisions, security overhead, etc. Traditionally, due to limited resources, nodes were tasked with only collecting measurements and sending them to a base station or central unit for processing. With increased capabilities of microprocessors the data processing is pushed more toward network and its more capable nodes. This thesis focuses to virtualize the processing resources of the entire network and dynamically distribute processing steps along the routing path while optimizing performance. Additionally, a new multi-key encryption (MKE) scheme is proposed to optimize efficiency while enhancing security. The main benefit of the MKE scheme is the improved resilience of the advanced encryption standard (AES) against correlation power analysis (CPA) attack by breaking the correlation between power consumption and the used secret key. The MKE security scheme is analyzed with network implementation and studied for its effects on network parameters such as network connectivity, resilience against node capture and energy efficiency of the scheme. Moreover, a new analysis methodology is proposed to quantify a resilience of a network against node capture such that the strength of the underlying security mechanisms is taken into account. Furthermore, the tradeoff between security and network performance is addressed by the proposed task-scheduling scheme. Also, the proposed methodology does not make assumption of homogenous network that is often used in literature to simplify analysis and scheme design. In contrast, the proposed formulation is generic, thus allowing heterogeneous nodes to be used while guaranteeing network performance. Consequently, the proposed scheme creates a wireless “computing cloud” where the processing tasks are dynamically assigned to the nodes using the Dynamic Programming (DP) methodology. The processing and transmission decisions are analytically derived from network models in order to optimize the utilization of network resources including: available energy, processing capacity, security overhead, bandwidth etc. As a result, the online optimization of network resources is achieved.

ACKNOWLEDGEMENTS

I would like to express my gratitude to my advisor, Dr. Maciej Zawodniok, for his guidance, supervision and encouragement throughout my graduate studies and with my research. His suggestions and supervision have provided important impetus for this research.

I also would like to thank Dr. Ann Miller and Dr. Yahong Rosa Zheng for their time and effort in serving as committee members and helping through my graduate studies.

Lastly, I am obliged to my parents, my sister, my brother-in-law, and my friends who have been very supportive throughout my studies offering encouragement. Without their help, I would not have been successful.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

LIST OF TABLES

1. INTRODUCTION

Objective

The main goal of this work is to improve the performance of wireless networks and applications, which are dependent on several factors including energy available at the nodes, channel capacity, security requirements, processing capacity at the devices, etc. The proposed scheme is designed to address these constraints while maximizing network performance in terms of energy efficiency, network lifetime [1], security of a data transfer, reduced network bottlenecks [2], etc.

Advantages

The proposed approach introduces new modeling and analysis methodologies to improve understanding of the network performance and its constraints. The proposed scheme for distributed processing is generic and designs to be an online solution. This initial work simplifies certain aspects of network control, specifically the routing is assumed to be formed before the task scheduling begins. However, the generic framework can easily be extended, in the future, to address other network dynamics and encompass complexity of networked application.

Motivation

The motivation behind this work is of two-fold:

- Energy efficient transmission and processing of data in the wireless network
- Improvement of the network security with emphasis on correlation power analysis (CPA) attacks

Multi-hop wireless networks relay data through intermediate nodes. The route through such a network is often constructed dynamically. Traditionally, wireless networks only store and forward the data to the destination while letting the application layer process the data at either source or destination. However, such an approach leads to high processing overhead at the end-nodes while the intermediate ones sit idle thus leading to unbalanced resource utilization, battery depletion, increased delay, etc. Consequently, many wireless and mobile applications would benefit from dynamic scheduling of data processing tasks while they are in transit. For example, instead of waiting until destination node to analyze the data, the processing can be distributed along

the route thus delivering the digested information to the destination. Such information can be used immediately without waiting for processing to end.

Moreover, wireless networks employed in a wide range of military and civilian applications including battlefield surveillance border and fire monitoring, traffic control, healthcare, voice communication, and body sensor networks. The requirements and constrains vary significantly among such applications. For example, a time-critical application favors a low end-to-end delay. In contrast, better energy utilization is preferred in case of battery operated, long-term monitoring application. Consequently, it is desired that communication protocols are aware of application demands and adopt themselves according to user requirements, which in turn depends on application needs. Overall, the proposed scheduling of a distributed processing is applicable to any of the wireless communication systems including wireless ad hoc, sensor and mesh network.

Some applications, for example surveillance or military ad hoc networks, require increased security services. However, due to remote deployment the wireless devices are often susceptible to capture by an intruder. The attacker will attempt to acquire secret information, for example secret keys used for data encryption. A correlation power analysis (CPA) is a very “attractive” type of attack since the attacker does not have to tamper with the device itself thus avoiding detection. The CPA attack passively monitors energy consumption in order to discover secret key employed by the node to encrypt data. The existing approaches to thwarting CPA attack, for instance heterogeneous S-Boxes which is discussed in Paper 2, focus on security alone while ignoring energy costs of the proposed solution. In contrast, the proposed MKE scheme addresses both security and energy-efficiency challenges of AES encryption in wireless networks.

Moreover, the impact of the security mechanisms on the overall network performance and resilience is often not adequately analyzed in the existing literature. In contrast, the presented work introduces a new methodology for analyzing the network connectivity and resilience when a specific security mechanism is employed. Additionally, the impact of the energy-efficiency of the encryption architecture on the distributed processing scheme is studied.

Furthermore, the required security level increases over time with the computational power available to attackers. The ever-improving processor’s speed and

capabilities that are available to the attacker force the application and network designers to increase the size of encryption key as the obvious remedy. As a result, the cost and energy consumption of the networked devices increases. Consequently, a simple increase of key size may not be sufficient to handle the tradeoff between the security, energy efficiency, and cost.

Approach

The proposed approach aims to schedule the processing of tasks among the nodes in the route to optimize the user defined metric, for example energy efficiency, delay etc. Easy adaptation of solution to application requirements by adjusting cost gains/metric. The proposed scheme improves the performance of the network by distributing the data-processing load within the network similar to cloud computing methodology. Cloud computing cost-analysis is utilization-oriented, and changes constantly to cope with changing requirements of users. This methodology when applied online to wireless networks will handle the distribution of tasks by the network nodes and thereby reduce the transmission costs and processing oriented delay costs. For example, a node can take a decision to process the data entirely by itself or partially process it and transfer it to the next available neighbor for further processing.

The proposed performance improvement approach employs a dynamic programming (DP) [3] methodology to analyze the tradeoffs with respect to application requirements including delay [4], security overhead, energy consumption [5], and nodes' capabilities. The derived communication protocol guarantees high performance in terms of the user requirements.

The proposed dynamic programming solution controls the energy consumption [6], the delay associated for processing a task by adjusting or managing the way the task is processed in the network. The proposed scheme based on DP model also examines how security overhead which acts as a burden (i.e., due to security architecture implementation) can be used along to improve the performance of the network in terms of energy efficiency, reducing end to end delay [7] etc. Hence, performance improvement scheme based on DP model could be employed in a wireless network to improve performance of wireless networks.

However, when a strong encryption mechanism is employed it increases energy consumption. As a result, the performance of the proposed task scheduling scheme will be reduced when an energy inefficient security mechanism is employed. In order to minimize the negative effect of such strong encryption mechanism the proposed DP approach uses multi-key encryption (MKE) [8] scheme to encrypt the data packets. The proposed novel MKE scheme thwarts correlation power analysis (CPA) attacks [9] [10] on advanced encryption standard (AES) algorithm while reducing energy overhead of the encryption mechanism. Consequently, the performance of the proposed DP-based network scheme is optimized while reducing energy expenditure and increasing security for data in the network.

For example, sensors communicate to exchange data using shared common keys to encrypt the transmitted data and it is made possible through cryptographic keys as well as key management protocols [12][13][14] to dictate the security infrastructure for sensor networks. Existing key management schemes have drawbacks with respect to at least one of network constraints including vulnerability of sensor nodes to attacks, resources of computation, communication, storage and power supply. Hence, it is important to maintain a good balance between the security and performance under constraints depending on application requirements.

The proposed scheme is evaluated in realistic networked scenarios. The metrics include the energy efficiency, network connectivity, and network resilience [16] [17] against node capture. The analysis results of the proposed scheme are generic thus can be applied in various communication networks with AES as encryption algorithm, to improve security against CPA attacks.

Finally, this combined methodology is analyzed how the focus on single metric would affect network in terms of other network factors. For example, focus on equal energy consumption distribution will affect delay associated with processing of a task and vice versa. The scheme is also analyzed in terms of various routing patterns in the case of heterogeneous nodes and in the case of mobile nodes in the network.

Contributions

Paper I:

- Proposed a communication model to evaluate the tradeoff between the execution of data processing tasks and delegating the execution to the neighbor nodes
- Developed a DP-based solution to evaluate tradeoff between user defined metrics to formulate appropriate decision
- Mathematical analysis of the scheme that provides guarantee of the performance for a generic wireless network, and can be applied to WSNs, wireless ad hoc networks, etc.

Paper II:

- Developed a novel, multi-key AES-based engine and protocol for wireless networks that thwarts the CPA attack while reducing energy consumption,
- Theoretical and simulation analysis of the proposed encryption scheme in terms of resilience to CPA and brute force attack that provides performance guarantee,
- Proposes a new methodology for analyzing a network resilience that consider the strength of underlying security mechanism

Future work

The proposed DP solution has to evaluate the effects of scheduling of tasks on available routes at a given point in the network. The effect of routing decisions on various performance-centric metrics has to be studied. The proposed DP-based solution uses Riccati equations that assume a simplified, linear system. Hence, an integrated and optimal control law for the task scheduling scheme has to be designed such that a complexity and nonlinear dynamics of wireless networks are addressed. The existing MKE protocol has to be extended to include a key management scheme for wireless networks for practical implementations since the existing schemes might incur high costs in terms of memory usage or key setup overhead.

PAPER

I. A DYNAMIC PROGRAMMING APPROACH: IMPROVING PERFORMANCE OF THE WIRELESS NETWORKS

Sandeep Kolli and Maciej Zawodniok
Department of Electrical and Computer Engineering
Missouri University of Science and Technology, Rolla, MO-65409
skkw8@mst.edu and maciej_zawodniok@ieee.org

ABSTRACT— Traditional wireless networks focus on transparent data transmission where data are processed at either source or destination nodes. In contrast, the proposed approach aims at distributing the data processing among the nodes in the network thus providing higher processing capability than a single device. Moreover, energy consumption is balanced in the proposed scheme since the energy intensive processing will be distributed among the nodes. The performance of a wireless network is dependent on number of factors including an available energy, energy-efficiency, data processing delay, transmission delay, routing decisions, security architecture etc. Typical existing distributed processing schemes have a fixed node or node type assigned to the processing at the design phase, for example a cluster head in wireless sensor networks aggregating the data. In contrast, the proposed approach aims to virtualize the processing, energy, and communication resources of the entire heterogeneous network and dynamically distribute processing steps along the communication path while optimizing performance. Moreover, the security of the communication is considered as important factor in decision to either process or forward the data. Overall, the proposed scheme creates a wireless "computing cloud" where the processing tasks are dynamically assigned to the nodes using the Dynamic Programming (DP) methodology. The processing and transmission decisions are analytically derived from network models in order to optimize the utilization of the network resources including: available energy, processing capacity, security overhead, bandwidth etc. The proposed DP-based scheme is mathematically

derived thus guaranteeing performance. Moreover, the scheme is verified through network simulations.

Keywords— Wireless sensor networks (WSN), Dynamic Programming (DP), Load Balancing, cloud computing

1. INTRODUCTION

The wireless networks have many military and civilian applications including battlefield surveillance, border and fire monitoring, traffic control, and healthcare and body sensor networks. Designing a durable sensor network has always been a challenge due to limited energy available at battery-operated devices. Moreover, in sensor networks a typical application has to extract information from the raw data. Typically, the information extraction is tasked to the sink node in order to conserve energy of sensors. However, the sensor devices are equipped with ever more capable processors. Additionally, the amount of extracted information is typically much smaller than the amount of raw sensor data. The energy consumption and the communication delay are proportional to the amount of transmitted data. Hence, the network-wide energy consumption and end-to-end delay can potentially be reduced when the data are processed early at the routing path. The proposed cross-layer optimization will dynamically optimize the performance of the networks in different areas: network routing [2], avoiding energy holes [3], prolong network lifetime [4] and others.

A number of related algorithms have been proposed for different application environments. In hierarchical-based algorithms [5][6], nodes are partitioned into different levels such that sensing data is transferred from lower to higher, up to the users. In wireless sensor networks, applications will have different requirements for data collection and dissemination process. For example, a network metric can be short packet delay for time-critical applications. In contrast, better energy utilization is preferred in case of battery operated, long-term monitoring application. Hence, it is essential that communication protocols are aware of application demands and adopt themselves according to application-requirements. The aim of the proposed model is integration of application requirements in terms of delay associated, security overhead, energy consumption and nodes' capabilities and design a communication protocol for better functioning of the network in terms of user requirements.

The proposed scheme improves the performance of the network by distributing the load within the network similar to cloud computing methodology. Cloud computing cost-analysis is utilization-oriented and adapts to changing application demand, topology,

and resource availability. In a traditional computing cloud, multiple applications are hosted on common set of servers, which allows consolidation of application workloads on smaller number of servers for better utilization. The clouds virtualize resources for example using virtual machines (VM) in order to efficiently distribute and quickly process multiple user requests. For example, a user starts a processing-intensive image manipulation application. Instead of spending hours on a local desktop or transferring to a specific super-computer, the application is inserted into a VM and sent to the cloud to be executed. The user's VM is dynamically assigned and if necessary distributed on physical machines inside the cluster without the user intervention or awareness. The computing cloud is capable of efficient load balancing and optimization of delay and energy-efficiency beyond what a manual operation would accomplish.

A task scheduling problem in the case of cloud computing deals with to meet user's job QoS requirements and use cloud resources effectively in an economic manner. However, nodes in a decentralized wireless networks have to collaborate among themselves to broadcast requests and route data. For example, typical battery-operated sensor nodes have limited energy supply that limits their lifetime. Hence, such a network has to optimize available resource in order to increase its lifetime, energy-efficiency, response time, etc. The proposed approach employs the concept of virtualization of resources and virtual machines (VMs) to manage the processing task. However, in contrast to traditional, wired computing clouds the wireless variant requires consideration also for communication costs and overhead. The mobile VM calculates the percentage of task to be completed at a particular node based on the resources available in the network. This methodology applied to sensor networks manages the distribution of tasks among the mobile nodes while reducing the transmission and processing oriented costs including energy and delay metrics. For example, a node can make a decision to either

- Execute entire set of tasks by itself and relay the final result (typically smaller than the input data set),
- Perform some tasks and transfer partial results to the next available neighbor for further processing, or
- Only transfer the data (and tasks) to the next node.

The proposed scheme also examines how a security overhead impacts the performance of the network in terms of energy efficiency, end-to-end delay, task distribution, network lifetime, etc. In order to minimize the security overhead an MKE [1] scheme is adopted for security. The MKE thwarts CPA attacks in wireless networks while reducing energy consumption. Overall, the proposed scheme aims to improve the performance of wireless network considering various metrics that impact the performance.

The proposed scheme is studied with respect to various cost optimization metrics using either single or multiple metrics. For example, focus on equal energy consumption distribution will affect delay associated with processing of a task and vice versa. The scheme is also analyzed in terms of various routing patterns of heterogeneous nodes and mobile nodes in the network.

In this paper, a mathematical model based on dynamic programming [7] is used to solve the issue of multi-stage decision-making. The decision to perform the task at particular stage or node of the network depends on various factors as described. Using DP methodology the multi stage decision problem is translated to multiple single stage problems that are correlative and solved accordingly.

2. BACKGROUND AND RELATED WORK

Optimization of a multi-hop wireless network is most naturally approached using dynamic programming (DP) methodology. Many researchers used the DP methodology in networks to solve various problems including finding optimal routing strategies, minimal energy consumption, optimal strategy in data aggregation, hierarchical routing issues, etc. W. G. Yang [8] proposes a DP based strategy where a minimal hop number with minimal energy consumption routing algorithm. However, designing a minimal energy consumption routing hasn't been considered. A. Ciancio and A. Ortega [9] considers optimal strategy sequence of data aggregation using DP principle to get a balance between energy consumption and data distortion. Using DP principle hierarchical routing is addressed in [10][11].

A dynamic programming optimization method was used in [12] to obtain an optimal scheduling policy that explores the channel dynamics to obtain a reasonable tradeoff between the communication throughput and packet transmission delay. A general DP framework was presented in [13] to obtain the optimal power and rate control policies that satisfy deadline-based QoS constraints. The DP approach was used in [14] to find a smart policy for energy-efficient tracking in wireless sensor networks. Based on DP approach, an algorithm was proposed [15] for a data-collecting sensor network, where the energy consumed includes both the transmission energy and energy consumed in the electronic circuitry.

A new metric-based cost function model is proposed to improve the performance of the sensor networks using DP principle. The DP solution yields distributed decision making at each node that minimizes the total cost function. De Couto et al [16] implemented a routing protocol that incorporates a metric called 'expected transmission cost' which measures expected number of transmissions required to successfully send a packet across a link. To optimize end-to-end delay and path capacity Draves et al [17] defined a two-term metric called 'weighted cumulative expected transmission time'. The first term accounts for end-to-end delay while the other accounts for interference. Iannone et al [18] defined the cost of a link as inverse of its nominal rate, and showed that by finding low-cost paths.

Dynamic programming technique is used for finding optimal route in wireless networks for reducing congestion, improving energy efficiency and for a variety of reasons. For example, Zhou [19] used DP methodology to find optimal routes in an energy efficient manner. However, the principle is not based on cost function which has been used the proposed scheme. It is more focused on considering nodes as states of the system, which rather simplifies than holistically solves the network performance optimization challenge. Similarly, Lingyang [20] using DP methodology to determine the best packet forwarding route that has maximum successful transmission rate subject to source-to-destination energy consumption constraint. It focuses only on energy consumption constraint but neglects other contributing metrics to improve performance of the network.

Using DP methodology many researchers aimed at finding optimal solutions for the network with respect to various metrics, for example length of routing path, security overhead, energy consumption, end-to-end delay, and throughput. The schemes improve the performance of the network with respect to only individual metrics. However, network performance depends on multiple metrics and it is essential to consider a combined approach. In this paper, a DP based approach is defined which improves performance of network in terms of energy utilization, balanced energy consumption in the network, reducing transmission costs and end-to-end delay. Moreover, the proposed scheme enables optimization of application-layer processing along the routing path which is lacking in existing literature.

In this paper, a cumulative cost function metric based on DP principle is proposed for WSNs. In this model, a communication model for the network is proposed to transform WSN structure into standard DP model. The cost function includes three metric terms: (a) residual energy available to the nodes, (b) delay, and (c) energy consumed for data transmission. Based on the cost function, node at each hop makes a decision on which processing tasks should be performed locally such that the user-defined metric is optimized.

The main contributions of this paper are: (1) a cost function for multi-stage decision making, (2) mathematical based communication model for WSN and (3) analysis of the proposed scheme with respect to each cost metric in theory and using

network simulations. The paper is organized as follows: communication model based on DP principle is presented in Section III. In Section IV, the cost analysis for communication model in presented and sub-optimal law for decision making of amount of data processing, security overhead and combination of all the metrics is presented. In Section V, the model is analyzed via simulation results with respect to metrics like lifetime of the network, cost of data transmission in terms of delay and energy.

3. COMMUNICATION MODEL

Typically wireless network follows the communication pattern where source nodes relay streams of data to a remote destination node either periodically or based on events. For example, a sensor node collects the measurements and transmits them to monitoring station where the data are processed. In typical WSN scenario, the nodes have fixed tasks to complete on their own with limited collaboration with other nodes in the network. The nodes perform the tasks regardless of resource availability at the node and its neighbors. This creates a divide within the network with nodes in the activity zone performing the tasks and depleting their own resources quickly. This leads to shorter lifetime of nodes and reduced sensing capabilities of the entire network.

In this paper, a communication model is proposed where nodes locally evaluate the tradeoff between the execution of data processing tasks and delegating the execution to the neighbor nodes. Moreover, the processing steps often reduce the amount of data that has to be forwarded to the destination. The scheme makes the decision based on the cost function that quantifies the energy resources on the nodes, individual nodes performance capabilities, processing delay including a task and cost of transmission of data between the nodes for completion of the task.

Additionally, the proposed scheme does not assume that all nodes are homogenous. In realistic scenario, some nodes may have higher processing capabilities thus should be preferred when assigning the tasks over other, resource constrained nodes.

Consequently, the communication model considers following four metrics when defining the cost function:

1) Energy Consumption: In WSN, energy available in the nodes is an important parameter in assessing the lifetime of the network. It is essential for better performance and to get desired results that all the nodes in the network would maintain same energy level. If some of the nodes in the network dissipate their energy quickly, then there is more chance of nodes dying earlier, thus rendering the sensor network ineffective. This metric will improve the lifetime of the network through balancing the energy levels among the nodes.

2) Cost of Transmission: This metric would help in assessing the cost associated with energy consumption for transmission of data packets and the associated delay, which are important metrics in time-critical applications. For example, to complete a task a node can either execute the entire task by itself or partially execute it and transfer the execution to the neighboring node with the data required to for completing it. In the first case, the transmission-energy is minimized since only the required information is communicated instead of much larger raw data. Also, the transmission delay is minimized since the least data has to be transmitted. In the later case, the task is divided among two or more nodes where partially processed data has to be forwarded between the nodes thus incurring higher transmission related costs (energy and delay). Hence, this cost metric will promote processing of the data early on the communication path.
3) Processing Delay Cost: This metric assesses the cost associated with processing of a task on a node in terms of delay time. In a network with nodes having varying capabilities some of the nodes can execute a task quicker when compared to other nodes. Hence based on user requirements or in time-critical applications communication model can be tuned in such a way this cost can be reduced in tradeoff with other metrics.
4) Security Overhead Cost: This metric would help in assessing the cost in terms of processing delay that would incur due to encryption and decryption of data at every node. This metric also measures the cost which incurs due to change in routing patterns due to problems in sharing a common key for communication between nodes. It is the cost which is the sum of processing delay and rerouting delays in the network. This metric would incur an additional cost in terms of energy consumption for encryption and decryption of data.

Remark: The above classified costs can be merged into one another and can be described as few costs governing the performance of the networks. For example, cost of transmission can be merged in energy consumption and processing delay costs. The above classification is done for better understanding of costs that would affect the performance of the networks. However, in simulations these costs are processed altogether.

The multi-decision metric vector is processed using dynamic programming principle in solving multi-stage decision-making.

Dynamic Programming Model

With respect to networking the DP model often assumes discrete stages that correspond to routing hops, while the decision is selecting an appropriate next hop among alternative routing options. In contrast, the proposed dynamic programming solution assumes that the route is already established and the decisions are about processing and transmission of the data along the path. The DP solution evaluates tradeoff between the energy consumption and delay in order to make the decision. Overall, the recursive solution to the proposed DP formulation renders a distributed scheduling of processing tasks along the established route such that the user-defined cost is optimized. In more general formulation, also the routing decision may be included in the DP decision-making process.

The proposed DP formulation uses following terms to describe the networking scenario:

5) **Stage**: The network is divided into a set of stages in the form of hops on the path or link indexed by positive integers
6) **State**: At each stage k, the state vector consists of two components - position of current node and decision vector. The state space is two – dimensional continuous space represented with min to max cost values to other stages from the current stage.
7) **Decision**: This part of model is critical in defining the decision at stage N based on the cost function values from the state space and representing the target position stage (N+1).

The communication model based on DP principle is defined mathematically and the cost function is calculated as cumulative costs incurred along the communication path. The next stage is selected based on the current state of the network and the decision vector, which is expressed as:

$$J(x(N+1)) = f(J(x(N)), u(N), q(N)) \quad (1)$$

where q(N) defines the current state of the network and u(N) defines the decision vector.

The u(N) is vector which is a combination of several metrics when described in mathematical terms is

$$u(N) = \{u_1(k), u_2(k), u_3(k), u_4(k), u_5(k)\} \quad (2)$$

where $u_1(k)$ – energy available on the nodes, $u_2(k)$ is the data transmission cost in terms of delay and energy spent, $u_3(k)$ is alternate routes to the target node, $u_4(k)$ is higher processing capability nodes, and $u_5(k)$ for security overhead.

1) Feedback mechanism

Let's consider a routing path that consists of a set of nodes. When making the decision about processor or forwarding, the local node needs to understand the capabilities of the remaining nodes in the path. Consequently, feedback information has to be relayed in opposite direction to the data flow.

Fig 1 illustrates the feedback mechanism in the network for communication for cost analysis. Nodes in the network communicate the necessary information for decision-making which is appended to ACK frames without the necessity of additional communication procedures. Nodes transfer necessary information that is vital for the cost analysis and should describe the cost-to-go terms sufficiently to make the optimal decision.

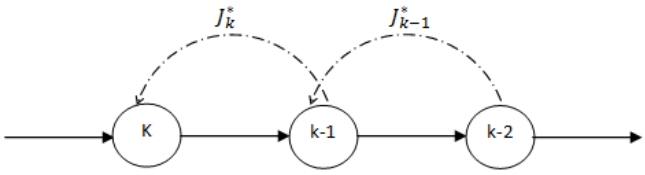

Fig 1. Feedback Mechanism of the Network

2) Cost optimization

In this subsection, the general description of the cost minimization is presented. First, the cost at the *k* state is defined as

$$\mathrm{J_N(x(N)) = Q_N(x(N)) + J_{N+1}(x(N+1))} \quad (3)$$

where $J_N(k+1)$ is the cost–to go for the next state. The DP scheme has to minimize the cost thus improving the performance of the network. In order to reduce the cost, it is calculated from the last state to initial state as defined below

$$J_N(X(N)) = Q_N(X(N)) \quad (4)$$

$$J_{N-1}(X(N-1)) = Q_{N-1}(X(N-1)) + J_N^*(X(N))$$

$$J_{N-1}(X(N-1)) = Q_{N-1}(X(N-1)) + f^{-1}(V(N)) \quad (5)$$

where V(k) is the information passed on to the previous states in the network; nodes in this case for cost analysis and appropriate decision making.

The proposed scheme based on dynamic programming principle improves the performance of the network in terms of improving the lifetime of the network, better utilization of nodes' resources and effective execution of the tasks. In contrast to traditional network scenario, this scheme improves quality of service in real-time application with limited communication overhead. The proposed DP solution dynamically assigns tasks in the network such that the cost function is minimized. The scheme is recursively applied at every node in the communication path. The minimal cost is calculated thus pointing the appropriate decision to either process data locally or delegate the processing task to the subsequent nodes. Consequently, the quality metrics in terms of delay and energy consumption are optimized since the DP scheme calculates the cost in terms of energy consumption for processing and data transmission, execution and transmission delay. Based on the cost function, an optimal policy has to be derived mathematically for reducing the cost and thereby guaranteeing an improvement of the network performance.

4. COST ANALYSIS

In this section, the mathematical model is analyzed in order to minimize the overall cost function such that performance of the network is improved. The proposed approach defines the cost function as

$$C(x_0) = E\{SE(x_N) + \sum_0^{N-1} SE(x(k), u(N)\} \quad (6)$$

where SE() is function which indicates the cost at each stage or node of the network and total cost is the sum of costs at target node and cost incurred between the source node and communicating node to the destination node.

The cost function in this model is the combination of individual cost variables

- Energy Dissipation Cost
- Cost of Transmission
- Processing Related Cost
- Security Overhead Cost

A. Energy Dissipation Cost

The energy dissipation cost is associated with the energy consumed by the processor to execute a task. In a heterogeneous network, each node will have different configurations in terms of resources available and its capabilities. The nodes in the network have to decide which processing steps should be executed locally. Moreover, the resulting collective decisions have to balance the load and optimize resource utilization. If only single node is tasked with all processing steps it will quickly deplete available energy (e.g. battery) thus reducing longevity of the network. Also, the nodes that have low, available processing capacity should limit the processing assigned to them since they will take significantly more time and resources to complete tasks.

For example, consider three nodes A, B and C in a network path. Data delivered to the user at destination node C have to be analyzed and processed. Consequently, each node has to decide about how much of the processing should be executed by it. The node A has to be processed and processing the data can be done entirely by A or partially process it and transfer the rest of the processing to either B or C. If the data is entirely is

processed at A then there would be no transmission cost because of no later processing involved at B or C.

If the entire process is done at A then the available energy at node A will be significantly lower than at the other nodes. Also, the high processing load will delay the execution of a next task scheduled for node A. If the task is appropriately distributed among nodes A, B and C then the delay costs will be balanced and uniform consumption of energy in the network is ensured. However, there is a cost of transmission of data involved but the cost can be optimized based on user's preferences accordingly.

In mathematical terms the dissipation cost would be the difference between the actual energy consumption to ideal consumption model where all the nodes dissipates energy in equal ratios.

$$\mathrm{E}\ (\mathrm{SE}\ (\mathrm{x_a})) = \mathrm{E_{ip}(N)} - \mathrm{E_{ideal}}$$

$$E(SE(x_a)) = \left[E_{ip}(N) - \left(\left(\frac{E_{current}}{\sum_{i=1}^{N} E_{inode}}\right) * (TEP)\right)\right] \quad (7)$$

where 'TEP' is the total energy consumption for execution of entire process and this metric defines how to uniformly utilize the nodes' energy resources all over the network and if this metric is higher then there is much difference in nodes energy levels which indicates non-uniform utilization of resources in the network.

B. Cost of Transmission

This cost is sum of two cost factors which incur during the transmission of data packets between the nodes. The energy spent for transmission of packets and the delay in sending the packets to the next processing node.

This metric is essential for uniform utilization of nodes resources in the network. It makes the process to be in a distributed way such that there is more chance of nodes sharing the burden instead of taxing a single node for entire process. However, there is cost associated in the form of transmission of data but it is overhead cost.

The cost of transmission is given by

$$C_{DP}\{SE(x_a, x_b)\} = \mathrm{C_{Trans}} + \mathrm{C_{Delay}} \quad (8)$$

$$C_{Trans} = (P_T.T_{st} + P_R.T_{st})$$

$$C_{Delay} = \left(\frac{\mathrm{L}}{\mathrm{D}}\right)$$

where P_T is the power used in the transmitter circuitry, P_R is the power used in receiver circuitry, L is the message length and 'D' is the distance between the nodes

C. Processing Oriented Cost

This metric expresses the cost associated with performing the task partially or completely at specific nodes based on their location or nodes hardware capabilities in terms of memory, speed of its processor, etc. Few applications require user requirements to fit in for performing specific tasks and may impart certain rules the way the task should be performed.

It requires the process to be completed at specific stages in the link which suits the user requirements. If this kind of metric has to be given a priority then it's a trade off to other discussed metrics.

$$C_{ps}\big(x(N+1)\big) = (x_{\mathrm{N}} - x_{ideal}) \tag{9}$$

D. Security Overhead Cost

This metric expresses the cost associated with implementation of security scheme in the network. The security scheme implementation results in an energy cost for encryption and decryption of the data and delay cost for encrypting and decrypting the data. It would also incur an additional delay cost in routing the data packets through a longer route in the case there is no direct communication between nodes because of no shared common key.

$$\mathrm{C_{SC}}\{\mathrm{SE}(\mathrm{x_a}, \mathrm{x_b})\} = \mathrm{E_S} + \frac{\mathrm{No\_cal}}{\mathrm{Sp\_proc}} + \left(\mathrm{k}.\frac{\mathrm{L}}{\mathrm{D}}\right) \tag{10}$$

where E_S is the energy consumption cost for data decryption and encryption, L being the message length transmitted between the nodes, D is the distance between the nodes, No_cal is the no. of instructions in the security scheme and Sp_proc is the capability of the node and k is the number of hops till the target node in a route.

E. DP Cost Optimization

The overall cost function considering the discussed cost metrics is given by

$$Total\ cost = [\alpha * \mathrm{E} + \gamma * \mathrm{C_{PS}} + \beta * C_{DP} + \delta * \mathrm{C_{SC}}] \tag{11}$$

Hence, the overall cost for the next stage can be calculated by

$$C_{OV}\big(x(N+1)\big) = E_i(x(N)) + C_{DP}(x(\mathrm{N})) + C_{ps}\big(x(N)\big) + \mathrm{C_{OV}}(\mathrm{x(N)}) \quad (12)$$

Theorem 1:

An optimal control law (21) using DP approach optimizes the energy-efficient distribution in the network

Proof:

The claim of the theorem is to state that it is necessary to minimize the cost associated at every stage in terms of energy consumption and efficient energy distribution amongst the network.

The state equation defined in terms of costs associated is

$$(\mathrm{C(N+1)}) = [E_i(\mathrm{N}) + C_{DP}(N) + C_{ps}(\mathrm{N})] \quad (13)$$

where E_i is the cost for energy consumed for a task and energy for transmission, C_{DP} is the cost for delay in execution as well as delay in transfer of data for the upcoming task and C_{PS} is the cost for deviation from effective implementation of the task in terms of user preferences.

Now an optimal control law is derived to optimize the energy consumption at every stage. The energy cost is defined as sum of data transmission cost and energy consumed for task execution.

$$C_T\big(P_o(k), V_i(k)\big) = U_i(k) + V_i(k) \quad (14)$$

The cost function (13) defines the transmission cost in terms of SNR because of power changes with change of modulation rate. Here $u_i(k)$ is the burst length, $P_i(k)$ is the power required for transmission of burst of data, SNR(r) and SNR(0) are signal-to-noise ratios for modulation r and 0 and R(r) is transmission rate for modulation r.

$$C_T\big(P_o(k), V_i(k)\big) = u_i(k).\frac{SNR\big(r_i(k)\big)}{SNR(0)}.\frac{P_i(k)}{R\big(r_i(k)\big)} + V_i(k) \quad (15)$$

where $V_i(k)$ is the energy cost for task execution. Calculation of optimal control law using DP will be highly computationally intensive. Instead an approximate quadratic function using Ricatti equation model [6] is derived.

$$C_T\big(P_o(k), V_i(k)\big) = \alpha_k . [P_o(k)]^2 + \beta_k . [Y_o]^2 \quad (16)$$

where $\alpha_k = \frac{SNR(r_i(k))}{SNR(0)} . \frac{u_i(k)}{R(r_i(k))}$ and β_k are constants which are used to approximate respective cost function in Ricatti equation form.

Remark: The cost function (14) will yield an optimal control law using DP. However, calculation of such law is intensive and sensitive to number of parameters such as $u_i(k)$. An approximated quadratic function is proposed (16) and α_k is selected such that error in least-square approximation is minimized [22].

The cost function is defined with the summation of both the defined costs and cost to go at k+1 state.

$$C_{ov}\big(Y_o(k)\big) = \alpha_k . [P_o(k)^2] + \beta_k . [Y_o(k)]^2 + C_{ov}\big(Y_o(k+1)\big) \quad (17)$$

Applying DP approach we have

$$C_{ov_N}\big(Y_o(N)\big) = \beta_N . \big(Y_o(N)\big)^2$$

$$C_{ov_k}(Y_o(k)) = min\big\{\alpha_k . [P_o(k)^2] + \beta_k . [Y_o(k)]^2 + C_{ov_{k+1}}\big(Y_o(k+1)\big)\big\}$$

$$C_{ov_k}(Y_o(k)) = min\big\{\alpha_k . [P_o(k)^2] + \beta_k . [Y_o(k)]^2 + C_{ov_{k+1}}(Y_o(k) + P_o(k))\big\} \quad (18)$$

First, the cost function is expanded for last iteration

$$C_{ov_{N-1}}(Y_o(N-1)) = min\big\{\alpha_{N-1} . [P_o(N-1)^2] + \beta_{N-1} . [Y_o(N-1)]^2 + C_{ov_N}(Y_o(N-1) + P_o(N-1))\big\}$$

$$C_{ov_{N-1}}(Y_o(N-1)) = min\{\alpha_{N-1} . [P_o(N-1)^2] + \beta_{N-1} . [Y_o(N-1)]^2 + \beta_N . [Y_o(N-1) + P_o(N-1)]^2\} \quad (19)$$

The minimization of above equation is done by differentiating it with respect to $P_o(N-1)$ and equating it to zero results in

$$P_o^*(N-1) = -Y_o(N-1) . \frac{\beta_N}{(\beta_N + \alpha_{N-1})} \quad (20)$$

By substituting (19) in (18) yields

$$C_{ov_{N-1}}\big(Y_o(N-1)\big) = L_{N-1} . Y_o^2(N-1)$$

where $L_{N-1} = \beta_{N-1} + \frac{\alpha_{N-1}.\beta_N}{\beta_N+\alpha_{N-1}}$ (21)

Following the above steps the optimal input for k=N-2,N-3,..0 can be calculated. The optimal control law for every k is given by

$$P_o^*(k) = -Y_o(k).\frac{\beta_{k+1}}{(\beta_{k+1}+\alpha_k)} \quad (22)$$

Hence, the optimal control law can be used for decision making for the amount the data processing that can be done at a node. This model can be used for other cost factors as well like end-to-end delay, security costs and a control law with all the contributing cost can be developed as well.

In the similar manner as above theorem formulated, the optimal control laws can be defined considering individual metrics or a control law considering every metric.

Corollary 1: Using DP approach the security overhead can be optimized.

Proof: This corollary deduced based on theorem 1 state that to optimize the security overhead and its impact on network performance metrics it is essential to guide the nodes in the network to utilize the security features according to the other performance metrics.

The state equation defined in terms of security costs is

$$C_{SC}\big(\rho_i(k), V_i(k)\big) = U_i(k) + V_i(k) \quad (23)$$

To calculate optimal control law is computationally intensive as in theorem 1, a sub-optimal solution based on ricatti equation is provided.

$$C_{SC}\big(\rho_i(k), V_i(k)\big) = \tau_k.\big(\rho_i(k)\big)^2 + V_i(k) \quad (24)$$

where ρ_i is derived from MKE [1] scheme which is defined from

$$\rho_{wH} = \frac{E(H(P)W) - E(H(P))E(W)}{\sigma(H(P))\sigma(W)} = \frac{a\sqrt{n}}{\sqrt{na^2 + 4\sigma_b^2}}$$

which gives the correlation strength of the key used for encryption based on the power consumption P.

$$C_{ov}\big(Y_o(k)\big) = \tau_k.[\rho_o(k)^2] + \beta_k.[Y_o(k)]^2 + C_{ov}\big(Y_o(k+1)\big) \quad (25)$$

Deriving in similar manner to theorem 1 gives control law as

$$\rho_o^*(N-1) = -Y_o(N-1).\frac{\beta_N}{(\beta_N+\tau_{N-1})} \tag{26}$$

Finally cost is defined as

$$\mathrm{C_{ov_{N-1}}}\big(\mathrm{Y_o(N-1)}\big) = \mathrm{L_{N-1}}.\mathrm{Y_o^2(N-1)} \tag{27}$$

where $L_{N-1} = \beta_{N-1} + \frac{\tau_{N-1}.\beta_N}{\beta_N+\tau_{N-1}}$

Corollary 2: Using DP an optimal control law can be derived for overall cost function.

Proof: This corollary is derived similar to the theorem 1. However, here all the costs involved in measuring the performance of the network are considered.

To derive the sub-optimal control law based on Ricatti equation with different metrics acting as different variables, all the other metric variables has to be transformed into some particular common metric. For example, every metric can be converted to a common metric, which is dependent on energy consumption.

The state equation defined for overall cost function is

$$\mathrm{C_T}\big(\mathrm{P_o(k)}, \mathrm{V_i(k)}\big) = \mathrm{U_i(k)} + \mathrm{V_i(k)} + \mathrm{\rho_i(k)} + \mathrm{S_i(k)} \tag{28}$$

In terms of ricatti equation methodology,

$$C_{ov}\big(Y_o(k)\big) = \alpha_k.[P_o(k)^2] + \beta_k.[Y_o(k)]^2 + \tau_k.[\rho_o(k)]^2 + \sigma_k.[L_o(k)]^2 + C_{ov}\big(Y_o(k+1)\big) \tag{29}$$

$$C_{ov}\big(Y_o(k)\big) = \min\{\alpha_k.[P_o(k)^2] + \beta_k.[Y_o(k)]^2 + \tau_k.[\rho_o(k)]^2 + \sigma_k.[L_o(k)]^2 + C_{ov}\big(Y_o(k+1)\big)\} \tag{30}$$

Metric variables- transforming them as single dependent metric variables

$$C_{ov}\big(Y_o(k)\big) = \min\{\alpha_k.[P_o(k)^2] + \beta_k.[Y_o(k)]^2 + \frac{\tau_k}{\alpha_k}.[P_o(k)]^2 + \frac{\sigma_k}{\beta_k}.[L_o(k)]^2 + C_{ov}\big(Y_o(k+1)\big)\} \tag{31}$$

$$C_{ov}\big(Y_o(k)\big) = \min\{\Big(\alpha_k + \frac{\tau_k}{\alpha_k}\Big).[P_o(k)^2] + \Big(\beta_k + \frac{\sigma_k}{\beta_k}\Big).[Y_o(k)]^2 + C_{ov}\big(Y_o(k+1)\big)\}$$

$$C_{ov_k}(Y_o(k)) = min\big\{T1_k.[P_o(k)^2] + T2_k.[Y_o(k)]^2 + C_{ov_{k+1}}\big(Y_o(k+1)\big)\big\} \tag{32}$$

Finally the control law is defined as

$$P_o^*(N-1) = -Y_o(N-1).\frac{T2_N}{(T2_N+T1_{N-1})} \quad (33)$$

where $T1k=\left(\alpha_k + \frac{\tau_k}{\alpha_k}\right)$ and $T2k=\left(\beta_k + \frac{\sigma_k}{\beta_k}\right)$

In this manner sub-optimal control laws is derived. As a result the performance of the network approaches the optimality, which is guaranteed analytically. In this paper, the cost function for the decision-making is considered as simple combined linear equation of all the discussed factors. The decision making is derived based on reducing the effective cost for task execution. Consequently, the associated cost is being minimized:

$$C_{OV} = \min\left[E_i\left(x(N)\right) + C_{DP}\left(x(N)\right) + C_{ps}\left(x(N)\right) + C_{SC}(x(N))\right]$$

$$C_{OV} = \sum_{i=1}^{N} \min\left[E_i\left(x(N)\right) + C_{DP}\left(x(N)\right) + C_{ps}\left(x(N) + C_{SC}(x(N))\right)\right] \quad (34)$$

$$C_{OV} = \sum_{i=1}^{N}[\min\left(E_{ip} - E_{ipide}\right) + \min(C_{DP} - C_{DPide}) + \min(C_{PS} - C_{PSide}) + \min\left(C_{SC} - C_{SCSide}\right)] \quad (35)$$

where E_{ipide} , C_{DPide}, C_{PSide} and C_{SCide} are the costs in the case of ideal situations. These costs would be related to cost of minimum of utilization of energy for the tasks by a particular node, cost of minimal transmissions required and cost of ideal implementation of the task in the network. These ideal costs are assumed when a network concentrates only on minimization of a particular metric.

$$C_{OV} = \sum_{i=1}^{N}[\min\left(E_{ip} - E_{ipmin}\right) + \min\left(P_T(T_{st} - T_{side}) + P_R(T_{st} - T_{side}) + \frac{L}{D}\right) + \min(C_{PS} - C_{PSide}) + \min\left(E_S + \frac{No_{cal}}{Sp_{proc}} + \left(k.\frac{L}{D}\right)\right)] \quad (36)$$

$$C_{OV} = \sum_{i=1}^{N} \alpha.[\min\left(E_{ip} - E_{ipmin}\right) + \beta.\min\left(P_T(T_{st}) + P_R(T_{st}) + \frac{L}{D}\right) + \gamma.\min(C_{PS} - C_{PSide}) + \delta.\min\left(C_{SC} - C_{SCide)}\right)] \quad (37)$$

where ‘α’, ‘β’, ‘γ’ and ‘δ’ are constants that have to be assigned with appropriate values to achieve the desired performance goal based on user’s preferences.

In the next section, the communication model is evaluated in terms of simulation with respect to lifetime of the network, energy spent on transmission, energy distribution in the network.

5. SIMULATION RESULTS

Simulation has been conducted in Matlab and NS2 to analyze the performance of the proposed communication mode in improving the performance of a wireless network. Table 1 summarizes the default network configuration, which is used unless otherwise specified.

Table 1. Parameter Settings of the Network

No. of nodes in the network	12
Link capacity	1 Mbps
Packet size	256
Attenuation coefficient	3
Min energy of the node in the network	34J
Max energy of the node in the network	92J

Nodes in the network are assumed to have following hardware configuration to simulate heterogeneous network with varying processing capabilities. The hardware profiles are

a. ARM based Beagle board [11] – 1200 MIPS, 673 mW at 600 MHz with energy consumption of 232nJ/Instruction
b. Missouri S&T mote – 100 MIPS, 115.5mW at 25MHz with energy consumption of 1.15 nJ/Instruction
c. ATmega 1282 – 242 MIPs, 16.5 mW at 4 MHz with energy consumption of 4 nJ/Instruction
d. ARM Thumb – 480 MIPS, 75mW at 40 MHz with energy consumption of 2.1nJ/Instruction
e. Cygnal C8051F300 – 32 KHz with energy consumption of 0.2nJ/Instruction and
f. IBM 405 LP – 152 MHz with energy consumption of 0.35nJ/Instruction

In the simulation, the wireless network with the proposed scheme is compared with traditional wireless network configuration. The network model is simulated for the proposed and traditional network configurations. The comparison analysis is performed in terms of network lifetime, energy distribution in the network over time, delay vs. density of the network, energy variation with weight based metric.

Remark: In the simulation, the entire data processing task is divided into sub tasks, which enables the distributed processing of the sub tasks at selected nodes. It is assumed that a subtask execution reduces the amount of output data when compared with the input data set size since the processing typically extracts essential information from the large set of raw data.

Fig 2 gives an idea of network topology with nodes placed in the network and indicated with the nodes' transmitting ranges. Nodes communicate among the network with the help of neighboring nodes to transmit data packets.

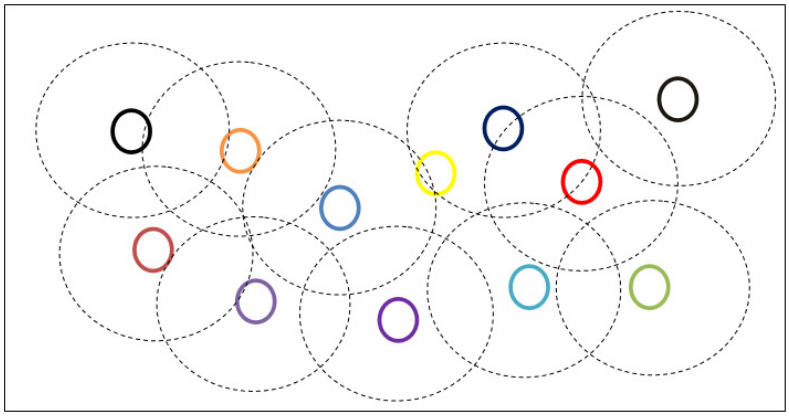

Fig 2. Example of Network Configuration

The nodes evaluate the tradeoff between processing a subtask and simple forwarding of unprocessed data. The analysis summarizes the cost incurred for completion of the entire task such that the cost function value is optimized. Fig 3 shows the total number of transmitted bits in the network for various scenarios.

The proposed scheme reduces the total number of bits transmitted among the nodes since it schedules the task dynamically to reduce the total cost which includes transmission cost that is proportional to amount of transmitted bits. Furthermore, this reduces energy consumption for transmission in the network thus increasing the lifetime of the network. Additionally, the proposed scheme reduces both: the delay associated with transmission and the total execution time of the entire task performed by the network. The upper and lower bounds in Fig. 3 illustrate the extreme cases when all processing tasks are executed either at the source or destination nodes alone. This processing of tasks at either extreme would correspond to a typical ad hoc wireless network scenario where the end nodes perform all the data processing and the intermediate nodes only forward data.

Fig. 4 illustrates the total energy consumption for both transmission and processing of the tasks. When the proposed DP-based scheme is employed the energy consumption costs with respect to data transmission as well as task execution is reduced when compared the costs incurred in traditional communication scenario where all data processing is performed by the sink node. Such a traditional network can be related to a WSN where the base station analyzes the sensor data while the sensors only relay the raw sensor data. This energy saving model improves the lifetime of the network and thus reducing deployment dollar-costs in terms of battery replacement, size of used batteries or solar panels.

Fig 5 illustrates variation of the lifetime of the traditional network in comparison to the proposed DP scheme based network model. As observed in Figs 2 and 3, the proposed scheme reduces energy consumption thus allowing longer operation of nodes wit hthe same amount of initial energy (e.g. stored in battery). Fig. 4 confirms that finding for the WSN network model. The presented lifetime of the network is an average over 10 simulations with random topologies which results in random order of heterogenous nodes on the comunication path.

Fig. 5 shows the the proposed DP-based scheme almost doubles the network lifetime. In the baseline case without the DP scheme, the entire network becomes inactive at time 125 due to energy depletion.

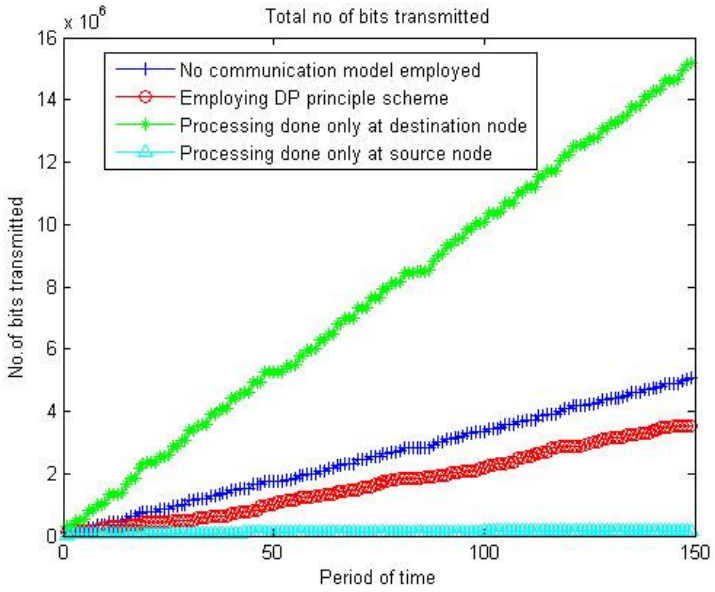

Fig 3. Total Number of Bits Transmitted

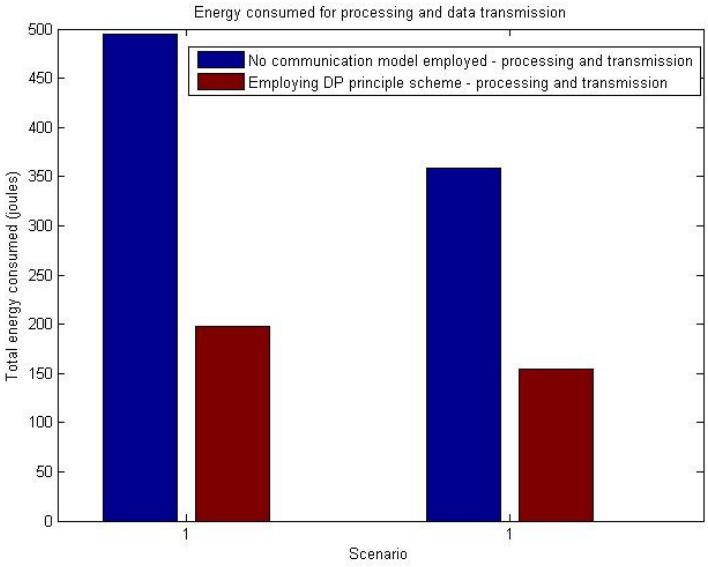

Fig 4. Energy Consumption for Task Execution and Data Transmission

In contrast, the proposed scheme ensures that a half of the network is still active. Also, the proposed scheme distributes the load such that the energy levels among the nodes are balanced. Consequently, larger number of nodes survive intil the end of the improved network lifetime when all the remaining nodes die almost simulataneously.

Fig. 6 illustrates the imbalance of available energy among the nodes in the network. The figure shows the difference between the maximum and minimum energy available at the nodes. A large difference indicates that there are nodes with very low and very high levels of available energy

The nodes with low available energy can die faster than the nodes with high available energy. Hence, this metric describes how well the scheme is balancing the energy consumption in the network. In the case of baseline network scenario without dynamic task allocation, the performance varies significantly and the difference increases with time thus indicating persistent imbalance that leads to more nodes dropping from network due to energy depletion

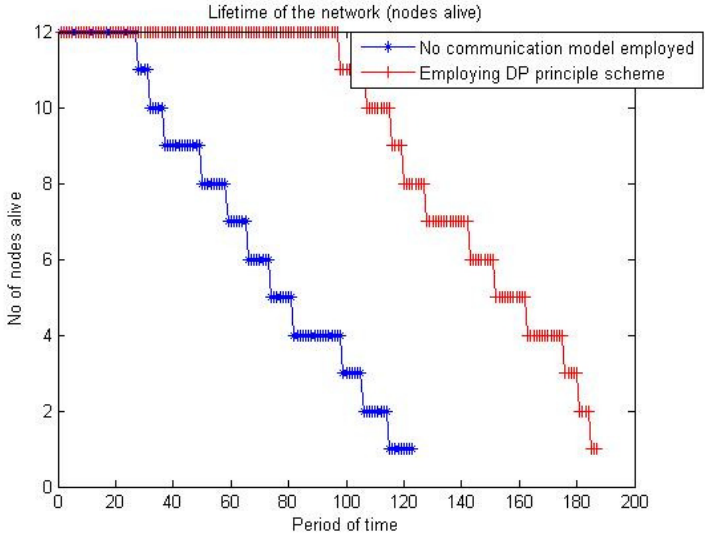

Fig 5. Lifetime of the Network (No. of nodes alive)

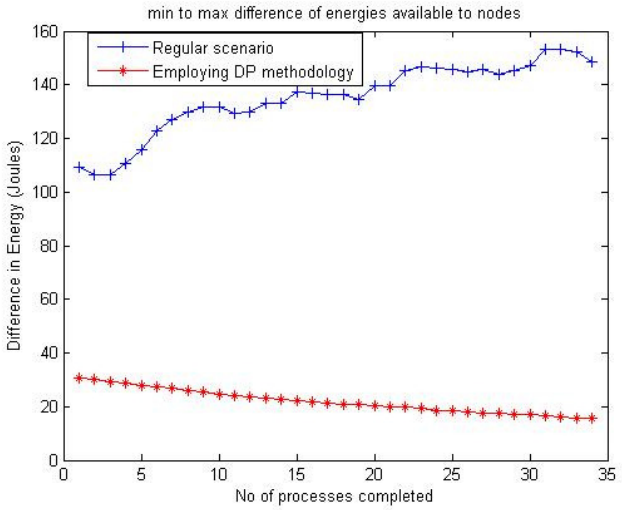

Fig 6. Min-Max Difference of Nodes' Energies

In the case DP based scheme the difference in energy available curve is gradually reducing since the task scheduling aims at reducing the imbalance. As a result, the entire network remains operational for longer period of time. Moreover, the better performance of the network can be guaranteed.

A. **Impact of Node Positions in the Network**:

In this section, the network is analyzed in terms of transmission and delay costs with respect to change in network topology based on node's capabilities. For example, the topologies are changed with high capability nodes - close to the source, close to destination etc. This analysis gives an idea how the network performance gets affected depending on the positions of the nodes in a heterogeneous network.

Fig. 7 illustrates the number of bits transmitted (cumulative) for various routing patterns. Four scenarios are presented where the nodes in the network are positioned based on their processing capabilities which are described in Table 2. In scenario 1, nodes with good capabilities are mostly used and placed close to source and destination and only few lesser capable nodes are placed. In scenario 2, very few high capability nodes

are placed in the network and in scenario 3 the ratio is even between high and low capability nodes. Scenario 4 is implemented with MKE security scheme.

Fig 7 shows that scenario1, high capability nodes perform most of the tasks with lesser data transfers since they can quickly process the data and need to transmit only the extracted information (smaller in size) to the neighboring nodes. In the case of scenario 2, network with less capable nodes, the nodes need to relay the information such that they can balance the load among themselves.

In the case of scenario 3, network with mixed capable nodes the data transfer is equally good as the case with less capable nodes because the scheme forces the nodes for equal available energy distribution.

In scenario 4, scenario 1 is repeated with security scheme MKE [1] and the data transmission is further reduced compared to scenario 1 because of additional security cost overhead. This security cost overhead which is the sum of energy, delay and routing costs has to be reduced which makes the proposed model to increase the processing of task at the nodes itself thereby reducing the security overhead cost.

Table 2. Network Topology Variation with Respect to Node's Capabilities

Scenario	Description
Scenario 1	High capability nodes close to source and destination
Scenario 2	Low capability nodes close to source and destination
Scenario 3	The ratio of number of high and low capability nodes equally placed to source and destination
Scenario 4	Scenario 1 with security scheme MKE

This reflects in lesser data transmissions between the nodes in the network. Finally, this analysis helps the user in determining the configuration of the network to his desired needs in terms of delay and energy efficiency.

B. Impact of Network Density on Delay Cost:

In this sub section, the impact of nodes' positions is analyzed in terms of delay cost with respect to change in network density and with security scheme MKE implemented in the network. The security scheme parameters are varied as shown in Table 3. The main aim of this analysis is to study the impact of density of the network on the delay cost with change in network topology and the impact of security scheme parameters on the delay cost as well. It is also analyzed for the scenario where the nodes are mobile.

Fig 8 illustrates the how the delays in the network between the source and destination nodes vary with respect to the change in density of the network. The simulation scenarios are described in Table 2.

Initially the delay is high due to limited number of nodes that can communicate among themselves. The MKE security scheme limits the communication to very secure links only, i.e. to links where the multiple keys are shared. In comparison, there might be multiple viable links that do not share enough keys.

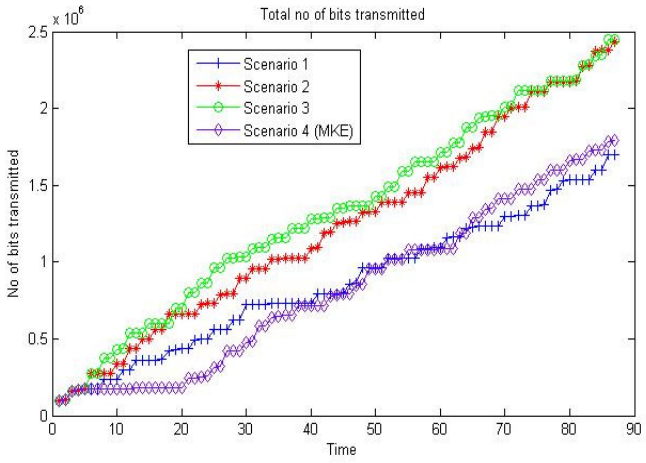

Fig 7. Total Bits Transmitted

Additionally, the network with low density forces the routing to use long routing paths. However, with increase in density more nodes would be able to communicate and delay reduces. If the density is increased above certain level the probability of more nodes sharing common keys increases with the chance of distributing the load among them. However, this increases the transmission delay costs in the network.

Fig 8 shows the delay cost higher in the case when nodes are mobile. This is due to the reason of security scheme which adds the routing cost because of unavailability of routes to destination nodes due to mobility. To reduce the cost the security scheme parameter T2 can be increased such that delay can be reduced with nodes having high probability of sharing common keys. This is a tradeoff which rests with user's specifications and can be determined accordingly.

Table 3. Impact of Network Density on Delay with Security Parameters (MKE) and Mobility

Scenario	T1	T2	T3	Description
Scenario 1	10	6	3	Varying network density with high capability nodes close to source and destination
Scenario 2	10	6	3	Varying network density with low capability nodes close to source and destination
Scenario 3	10	8	3	Varying network density with ratio of number of high and low capability nodes equally placed to source and destination
Scenario 4	10	6	3	Scenario 1 with mobile nodes
Scenario 5	10	8	3	Scenario 2 with mobile nodes
T1 - Number of keys in key pool T2 - Number of keys stored per node T3 – Number of keys required for communication				

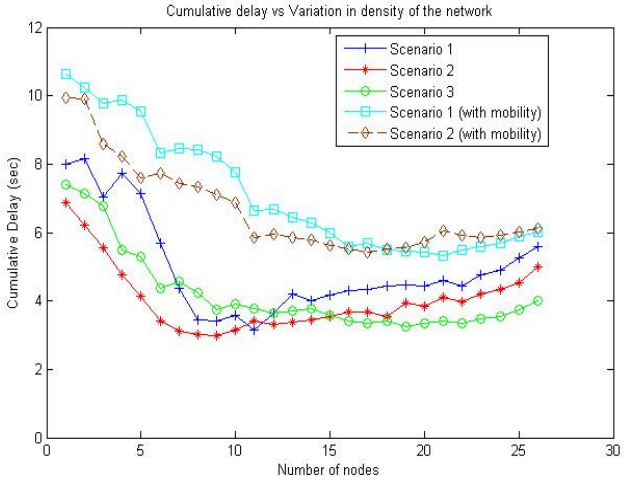

Fig 8. Cumulative Delay with Varying Network Density (MKE)

C. Impact of Weight Given to Metric on Energy Variation and End-to-End Delay:

In this section, the weightage given to metrics is studied for its impact on energy variation and end to end delay. This helps in user defining the metric weights according the application needs and gives a better flexibility in understanding and improving the performance of the networks.

Fig 9 illustrates available energy variation in the network based on the amount of weight assigned to the particular cost term (e.g., available Energy (E) and Delay (D)). The available energy for the nodes is affected by the task processing cost, security cost for encryption and decryption, and energy used for transmission. The delay metric includes the task processing delay, data transmission delay, security implementation delay, and rerouting delay. Fig. 9 shows the available energy distribution among the nodes in the link and the Fig. 10 illustrates the cumulative end-to-end delay.

In Fig. 9, for the scenario 4 (E=0, D=1.0) the energy available variation is stable because it is assumed that network dies if one of the nodes' available energy value crosses a certain minimum threshold. In this scenario, network dies and there is no further processing done. Hence, the variation value is constant. In Fig. 10, for scenario 4 the delay is constant because network dies at time (t=16) and no further processing is done. The cumulative delays are presented for different scenarios and depending on application user can define the respective weights.

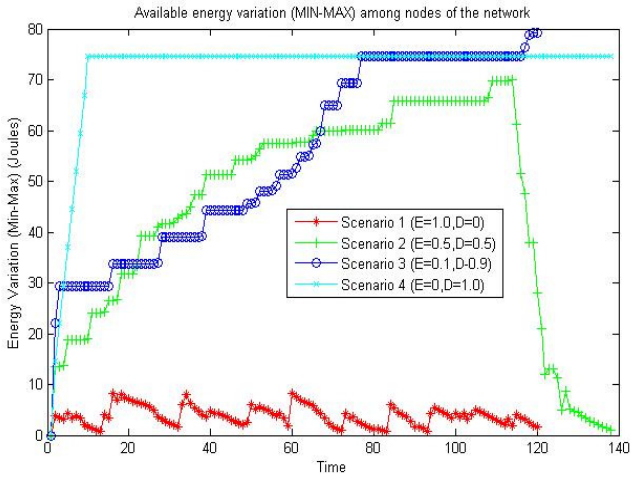

Fig 9. Available Energy Variation of the Network

The above network analysis illustrates the benefits of employing the proposed scheme in terms of energy consumption balancing and delay. Additionally, it provides guidance in selecting the appropriate parameter values for the particular application. This methodology based on DP scheme helps in effective governing of the system and defining the desired utilization of network resources by the system according to the user's requirements.

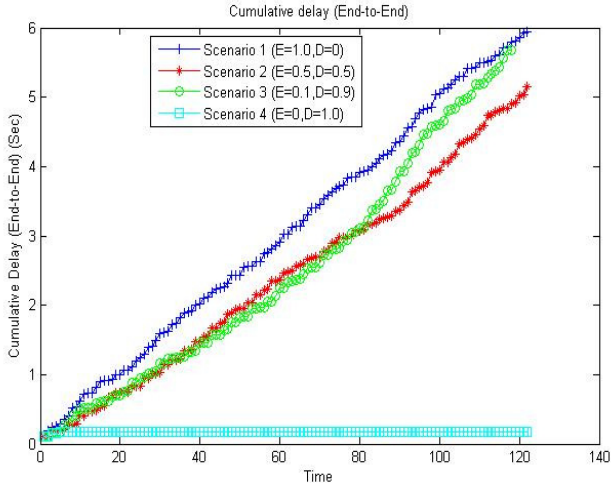

Fig 10. Cumulative Delay Variation of the Network

6. CONCLUSION

The proposed DP based communication and task-scheduling scheme improves the performance of wireless networks against regular WSN network scenario. It has reduced the energy consumption costs for the data transmission as well as processing cost by 65% and practically doubled the network lifetime. Also, it reduced the energy inequalities among the network thus improving utilization of the network resources.

Additionally, the communication cost in terms of delay is reduced since fewer bits have to be transmitted. Consequently, the communication bottlenecks have lesser effect on the quality of service. The proposed DP based communication model reduces the costs in terms of energy consumption and the overhead from the implementation of security scheme.

The proposed scheme helps in improving the performance of the networks from most of the network metrics perspective and it is not focused on improving a performance of the network from a single metric perspective.

7. REFERENCES

[1] Sandeep kolli, Maciej Zawodniok, "Energy-efficient multi-key security scheme for wireless sensor networks", 5th LCN workshop on Security in Communication Networks, Zurich, Switzerland. Proceedings of 34th IEEE LCN, 21-23 Oct 2009.

[2] R Yang Yu. Bhaskar Rrishnaiilachari. and Viktor K. Prasanna, "Energy- Latency tradeoffs for Data Gathering in Wireless Sensor Networks", IEEE 2004.

[3] A.E. Gamal, C. Nair, B. Prabhakar and S. Zahedi, "Energy-efficient scheduling of packet transmissions over wireless networks", IEEE Infocom, 2002.

[4] A. Manjeshwar and D.P. Agrawal, "TEEN: A routing protocol for enhanced efficiency in wireless sensor networks," Proc. Of 15th parallel and Distributed processing symposium, 2001.

[5] J.L. Williams and J.W. Fisher, "Approximate Dynamic Programming for communication-constrained sensor network management", Proc of IEEE Transaction on Signal Processing, Aug 2007 pp 4300-4311.

[6] W. Y. Ge, J. S. Zhang and G.L. Xue, "Cooperative geographic routing in wireless sensor networks," appears in the Proc. of 2006 Military Communications Conference, Oct 2006 pp 1-7.

[7] D. P. Bertsekas, Dynamic Programming: Deterministic and Stochastic Models. Prentice-Hall, Inc., Englewood Cliffs, 1987.

[8] W.G. Yang, T.D. Guo and T. Zhao, "Routing algorithms of the wireless sensor network based on dynamic programming", in Journal of Computer Research and Development, 2007, pp 890-897.

[9] A. Ciancio and A. Ortega, "A Dynamic Programming Approach to Distortion-Energy Optimization for Distributed Wavelet Compression with Applications to Data Gathering In wireless Sensor Networks," Proc of 2006 IEEE International conference on Acoustics, Speech and Signal processing, May 2006, pp 14-19.

[10] J. Cartigny, D. Simplot and I. Stojmenovic, "Localized minimum-energy broadcasting in ad-hoc networks," appears in INFOCOM 2003 Twenty- Second Annual Joint Conference of the IEEE Computer and Communications Societies, vol.3, 30 March-3 April 2003, pp 2210–2217.

[11] W. Y. Ge, J. S. Zhang and G.L. Xue, "Cooperative geographic routing in wireless sensor networks," appears in the Proc. of 2006 Military Communications Conference, Oct. 2006, pp 1-7.

[12] Gyouhwan Kim and Rohit Negi, "Dynamic programming for scheduling a single route in wireless networks", IEEE 2007.

[13] T. Holliday, A. Goldsmith, and P. Glynn, "Wireless link adaptation policies: QoS for deadline constrained traffic with imperfect channel estimates", in *Proc. IEEE ICC*, 2002, pp 3366–3371.

[14] J. Fuemmeler and V. V. Veeravalli, "Smart sleeping policies for energy efficient tracking in sensor networks," IEEE Trans. Signal Process, vol 56 no 5, pp 2091-2101, May 2008.

[15] Y. Yu, B. Krishnamachari, and V. K. Prasanna, "Energy-latency tradeoffs for data gathering in wireless sensor networks", in Proc IEEE INFOCOM, 2004, vol 1, pp 244-255.

[16] D. Couto, D. Aguayo, J. Bicket, R. Morris, "High-throughput path metric for multi-hop wireless routing", MobiCom 2003, San Diego, CA – USA.

[17] R. Draves, J. Padhye, B. Zill, "Routing in multi-radio, multi-hop wireless mesh networks", MobiCom 2004, Philadelphia, PA – USA.

[18] L. Iannone, K. Kabassanow, S. Fdida, "Evaluation of cross-layer rate aware routing in wireless network test bed ", Eurasip Journal on wireless communications and networking, vol 2007.

[19] Zhou Zeshun, Li Layuan, Xu Yi, Wang Xiangli, "An Energy Efficient routing Algorithm Based on Dynamic Programming in Wireless Sensor Networks", IEEE, 2009.

[20] Lingyang Song , Yan Zhang , Rong Yu , Wenqing Yao , and Zhuo Wu, "Cross-layered Optimized Routing for Wireless Sensor Networks Using Dynamic Programming", IEEE, 2009.

[21] http://support.intel.co.jp/pressroom/kits/core2duo/pdf/epi-trends-final2.pdf

[22] Maciej Zawondniok and Jaganathan Sarangapani, " Energy-Efficient Rate Adaptation MAC Protocol for Ad Hoc Wireless Networks", International Journal for Wireless Information Networks, Vol 14, Springer-Verilog, pp 251-263, 2007.

PAPER

II. ENERGY-EFFICIENT MULTI-KEY SECURITY SCHEME FOR WIRELESS SENSOR NETWORKS

Sandeep Kolli and Maciej Zawodniok
Department of Electrical and Computer Engineering
Missouri University of Science and Technology, Rolla, MO-65409
skkw8@mst.edu and maciej_zawodniok@ieee.org

ABSTRACT - This paper proposes multi-key encryption scheme and engine architecture (MKE) that increases security and optimizes energy efficiency of sensor networks, while minimizing modifications to existing implementations. The scheme improves security of AES against correlation power analysis (CPA) attack by employing MKE engine, breaking the correlation between power consumption and the used key. The MKE scheme in network implementation is studied for its effects on network parameters such as network connectivity, resilience against node capture and energy efficiency of the scheme. Maintaining connectivity as well as ensuring secure communication between entities is vital for achieving desired sensing activities. In the proposed scheme, the resilience against node capture is measured in a distinguished manner compared with existing schemes. The proposed metric to measure network resilience takes into account the principle of underlying mechanism which helps in measuring key lifetime and key compromise probability. This realistic approach gives better mechanism in understanding security attacks or improving security architecture for wireless networks. Both analytical and simulation results are presented for the MKE scheme against CPA attack, analytical analysis for network resilience and the schemes' network implementation in this paper.

Keywords— Wireless sensor networks (WSN), Advanced Encryption Standard (AES), Correlation power Analysis (CPA), key pre-distribution.

1. INTRODUCTION

The wireless sensor networks are increasingly employed in various applications, for example border security with sensors to detect intrusions, drinking water contamination detection around the water collection point. The secure communication in such networks becomes increasingly important. The system should prevent unauthorized access, tampering with the systems, and other malicious activities. However, the WSN poses several specific challenges related to security. First, a typical WSN consists of hundreds or thousands of battery-powered sensing devices. Hence, the sensor mote's cost and energy consumption have to be minimized in order to make the WSNs viable for commercial applications. Second, the limited processing capabilities prevent from utilizing complex and computationally intensive encryption algorithms. However, the required security level increases over time with the computational power available to attackers. Consequently, the ever-improving processor's speed and capabilities force the sensor designer to increase the size of encryption key thus increasing cost and energy consumption of the devices. Hence, a simple increase of key size is not suitable to handle the tradeoff between the security, energy efficiency, and cost requires a different approach.

Within a network, sensors communicate among themselves to exchange data and use a shared common key to encrypt the transmitted data. Due to storage constraints, it is infeasible to store a key for every other sensor in the network. Secure communication is made possible through cryptographic keys as well as key management protocols which dictate the security infrastructure for sensor networks. Many existing key management schemes have drawbacks with respect to at least one of network constraints like vulnerability of sensor nodes to attacks, resources of computation, communication, storage and power supply. Hence, it is vital to maintain a good balance between the security and performance under constraints depending on application requirements.

The proposed scheme employs multiple keys to improve the overall security. The proposed scheme uses these keys in a random sequence to encrypt a particular message. Hence, if attacker discovers a single key then only a fraction of the message is compromised. Consequently, all the keys have to be compromised before the link

becomes unsecure. Moreover, the order and the id of the particular key used are hidden from attacker since the keys are selected randomly and switched on a block-by-block basis instead of per packet or per link basis.

The proposed MKE scheme in network implementation achieves better resilience against node capture compared to few of the existing key management schemes. MKE scheme requires nodes to have multiple shared keys to have communication for packet transfer. In fact, multiple shared keys requirement impacts the nodes in terms of memory overhead and network connectivity. To achieve good network connectivity nodes should share more keys in common for communication and it effects the resilience of keys in the case of node capture. It is essential to maintain a balance between number of shared keys and connectivity of the network; dependent on number of keys stored per node, size of key pool from which keys are selected and number of keys required for communication.

The proposed scheme is evaluated in terms of how it impacts the connectivity of the entire network and how it improves the energy efficiency of the network. The proposed scheme can be applied in any communication network with AES as encryption algorithm, to improve security against CPA attacks. However, it is especially suitable to memory constrained, energy-limited wireless sensor networks.

Note: This paper is an extended version of the accepted publication [1]. In this paper, we additionally presented the network implementation of the MKE scheme and presented analysis in terms of network connectivity, resilience against node capture and energy efficiency. A new metric is presented to effectively measure network resilience and gives better insight in determining key lifetime and probability of key compromise. Both analytical and simulation results were presented.

2. BACKGROUND AND RELATED WORK

The proposed scheme aims at thwarting different attacks on AES algorithm while minimizing necessary changes to the encryption engine implementation. The scheme should be used in conjunction with a key distribution scheme that provides the nodes with sufficient number of keys. Many distribution algorithms [2][3] have been developed and can be used with the proposed scheme, for example Eschenauer and Gligor [4] have developed random key pre-distribution protocols in which a random subset of keys from a large pool of symmetric keys is loaded to each node have to find one common key from their subsets which will be used as shared secret key for protecting their communication. The Eschenauer-Gligor scheme has been progressively improved [5][6][7]. For example, Du et al. [6] proposed the DDHV (Du, Deng, Han, and Varshney) scheme. The DDHV scheme is based on a multiple key space scheme generated from Blom's [8] λ-secure symmetric key generation system, which is randomly assigned to each sensor node in the network. Schemes using random distribution of keys are proposed with different approach techniques to distribute keys among nodes based on different metrics like security, memory, and energy-efficiency. Also, similar mechanisms have been proposed for heterogeneous WSNs [9][10].

In general, sensor nodes will either have to be powered by small nonrenewable batteries or use a modest amount of energy harvested from the environment, for example from solar panel. However, the amount of available energy in both approaches is limited thus thwarting node operational capabilities. Hence, developing energy-efficient cryptographic algorithms and methods is a critical issue in designing protocols for wireless sensor networks, including the security schemes. Some existing studies suggest storing the master key in tamper-resistant memory to reduce the risk [11] [12]. However, there exist attacks that do not require direct access to the memory with the secret key. For example, CPA attack exploits knowledge of hardware implementation of AES to determine a key value using energy signatures.

Power analysis attacks pose a serious threat to implementations of cryptographic algorithms since the attacker does not have to gain access to protected memory. A practical power analysis attack method has been demonstrated [13] [14]. There exist

strategies to protect a device against such an attack, for example by masking the intermediate results [15]. However, the existing approaches often require significant modification to the encryption engines [16] and increase energy consumption [17]. For example, a set of different, energy-suboptimal S-Box implementations can be used to hide the key at the cost of higher energy consumption [18]. In contrast, the proposed scheme allows selecting the most energy efficient AES implementation while counteracting CPA attacks by rotating available keys. Each key has a different energy signature, thus breaking correlation between energy consumption and a key value. Hence, the proposed scheme ensures the CPA attacks fails.

This paper presents analysis of the security improvements of the proposed multi-key encryption scheme using the AES cipher. The AES is a symmetric block cipher standard, which was issued by the National Institute of Standards and Technology (NIST) in 2001 [18]. However, it has to be noted that the proposed scheme does not dependent on a specific cipher since the theoretical analysis does not assume usage of AES. Existing multi–key schemes aim at improving the security against the brute force attack by increasing the effective key length. For example the Triple-DES [19] uses the three keys on each block of data subsequently. In contrast, the proposed scheme counters both the CPA and brute force attacks by using a randomly selected key for each block. Consequently, the attacker does not have information which key was used to encrypt the particular block.

The proposed scheme [1] is considered for deployment as a key management scheme and verified in terms of network parameters like network connectivity and resilience against node capture. Existing management schemes [20][21][22] define the network resilience toward node capture by estimating the fraction of total network communications that are compromised by capture of ‘x’ nodes not including the communications in which the compromised nodes are directly involved.

Zhong [23] proposed a scheme where auxiliary nodes help in key establishment for network nodes and capture of auxiliary nodes is a major setback in resilience to this scheme. The resilience is calculated in this scheme based on analogy that compromise of normal nodes does not affect security. Sujan Li [24] proposed where nodes in the network are self classified into worker nodes and service nodes dynamically. In this

scheme the service nodes are not predefined and these are responsible for shared key establishment. The resilience is calculated given an attack radius, the fraction of all directly-compromised links among all the compromised links. Dijiang [25] proposed byzantine resilient multi-path key establishment scheme that uses the Reed-Solomon error correct coding scheme to improve resilience to byzantine attacks.

In MKE scheme, the resilience is assumed as combination of resistance offered in the capturing initial set of compromised nodes (against CPA) and resistance offered in compromising additional 'x' nodes to capture keys. The resilience differs with existing schemes because with the MKE scheme attacker required additional time or resources to capture keys from the nodes. The scheme is also verified in terms of energy efficiency of the network and compared with existing management schemes.

The main contributions of this paper are: (1) novel AES engine architecture that can utilize multiple keys to increase security, (2) theoretical analysis of the performance of the proposed scheme, and (3) a simple and energy-efficient hardware model for implementing the proposed scheme. The paper is organized as follows: in Section III, the main types of attacks on AES algorithm are discussed. Next, the proposed multiple-key encryption technique is presented in Section IV. In Section V, the theoretical analysis of proposed technique is given and analyzed in terms of network connectivity and resilience against node capture. In Section VI, the analysis of network resilience and network performance of MKE scheme is presented. Finally, the simulation results for power correlation attack, network connectivity and resilience against node capture are presented in Section VI.

3. SECURITY ATTACKS

In this paper, the performance analysis is conducted with regards to two types of attacks: (a) the CPA and (b) the brute-force attack on AES scheme. First the details of the attack technique are given, in order to gain understanding how the proposed scheme improves the security.

A. Correlation Power Analysis Attack

The CPA attack exploits the correlation between energy consumption of the circuit and the data processed on it. Often, it is assumed that the circuit's power consumption varies linearly with the bit-wise difference in the processed data [13][14]. For example, if a register bit changes value, the energy consumed is different than if the bit value does not change. For the particular S-Box design, the attacker can analyze correlation between power signatures and the pair of a plain text and a key. When the encryption is repeated for a sufficient number of plaintexts the statistical correlation with simulated keys can be calculated. The key with the highest correlation is considered to be the secret key. Moreover, this method is noninvasive since the attacker does no need to access and read the memory with the key, which often is protected [11][12].

Next, the analysis of CPA attack is performed for the partial key K_s for simplicity. However, the results are valid for the retrieval of the whole key since the method can be repeated to retrieve the other partial keys. For AES, the CPA attacker analyses power signatures for the first and last round of the encryption process. For the CPA attack, a predictable power consumption model is considered:

$$W_S(j) = \mathrm{W}\big(K_S, \mathrm{PT}(j)\big) \tag{1}$$

where $W_S(j)$ is the power consumption for plaintext j, K_S is a partial key, $PT(j)$ is the j^{th} random plaintext, and W is a function of power dissipation. Given N plaintexts, the predicted power $W_S(j)$ can be derived using (1), and the corresponding power traces calculated. In general, the CPA assumes that power consumption is proportional to number of bits changed in S-Box register. In other words, the power is proportional to Hamming distance [21]. To simplify the analysis while not losing generality, it is

assumed that the register, R is initialized to zero (0). Consequently, the power consumed can be expressed as

$$W = a \cdot H(D) + b \cdot D \tag{2}$$

where a is a scalar gain between the Hamming distance, H, and the power consumed, W. The current and previous states of the S-Box register are expressed as D and R respectively, b is power dissipation induced by noise offsets, and time dependent components in a 128-bit random key. If D contains m independent and uniformly distributed bits, the whole word has an average hamming weight $\mu=m/2$ and a variance $\sigma 2=m/4$. Hence, the correlation coefficient between W and $H(D)$ is equal to:

$$\rho_{wH} = \frac{E(H(D)W) - E(H(D))E(W)}{\sigma(H(D))\sigma(W)} = \frac{a\sqrt{m}}{\sqrt{ma^2 + 4\sigma_b^2}} \tag{3}$$

When a partial key guess, Ks, is considered then

$$P = PT_S \oplus K_S \tag{4}$$

where PT_s denotes the corresponding partial plaintexts. If PT_s contains n independent and uniformly distributed bits, it has an average $\mu=n/2$ and a variance $\sigma 2=n/4$. Consequently, the correlation between W and P is expressed as:

$$\rho_{wH} = \frac{E(H(P)W) - E(H(P))E(W)}{\sigma(H(P))\sigma(W)} = \frac{a\sqrt{n}}{\sqrt{na^2 + 4\sigma_b^2}} \tag{5}$$

According to above discussion, the partial key guess is correct, if the intermediate results and the power consumption are correlated, that is the highest correlation coefficient is achieved for that key.

B. Brute Force Attack

The brute force attack is a simple type of attack though requires relatively large effort. The attacker decrypts the cipher text trying every possible key. Assuming the attacker can identify if the decrypted value is the correct ones, the technique requires on average to decrypt half of the total number of possible keys. Hence, for a sufficiently long key the brute force attack becomes impractical. However, the ever-improving performance of modern processing systems quickly ages and weakens the security of AES for a given key size, as shown in Table 1. Simple remedy is to increase key size in par with technical capabilities of a potential attacker. However, in case of resource

limited sensor nodes the added memory, processing, and power requirements become prohibitive.

Current practice is to use a 128-bit AES key. Hence, the total number of different keys is equal to 3.4×10^{38}. Table 1[1] illustrates how long it takes to break the AES key using brute force attack. The current results are contrasted with the results from 1995. Additionally, Table 2 [1] shows the decrease in hardware costs per 1000 (millions instructions per second) MIPS [19][20]. Hence, it can be inferred that the security of the AES decreases with time for the same key size.

In conclusion, a simple remedy of increasing key size might increase security against brute-force attacks but for WSNs due to resource limitations in terms of memory, battery power a different approach is needed. The security of the proposed scheme increases without need for larger encryption engines. The analytical results are presented in Subsection 0.

4. MULTI-KEY ENCRYPTION TECHNIQUE

The proposed encryption scheme utilizes multiple keys to encrypt plaintext using AES algorithm. The subsequent blocks of plain text are encrypted using randomly selected keys. In contrast, the standard AES uses a single key to encrypt the whole plaintext. The proposed scheme increases security when compared with the single key approach since complete decryption can be done only with all utilized keys.

The proposed scheme provides uniform security to all data, it is possible to vary the security level (e.g. number of used keys) based on requested protection. In such cases, MKE scheme can be adjusted to use more number of keys for high priority data and fewer keys for low priority data.

The packet is encrypted such that only the destination node can decrypt the data with the corresponding shared keys. The original message is pre-pended with two fields: the first key ID and a seed, as shown in Fig. 1.

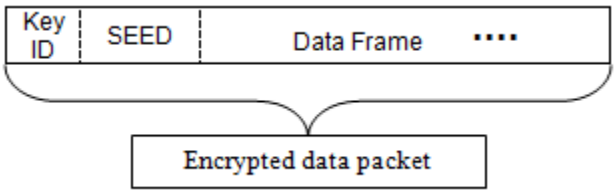

Fig 1. Data payload of a packet

A. Synchronization of Radom Key Sequences

The Key ID and seed fields are utilized for the synchronization purposes. When the destination receives the message it needs to first *synchronize the pseudo random generator* with the source in order to discover the appropriate sequence of keys. Hence, the first block of the message is decrypted using each shared key until the correct key is found, that is when the message's key ID matches the one of the applied key.

When the right key is found for the first block the subsequent blocks are decrypted only once using the correct sequence of keys selected by the pseudo random generator. Also, the same random generator is applied for the subsequent messages in order to reduce the overhead of trying all the shared keys for the first block of every message.

Moreover, the loss of synchronization between transmitter and receiver, for example due to lost packets and retransmission, can easily be detected. The receiver node compares 'key id' and 'seed' fields from each message with the random generator sequence. The match confirms a successful synchronization and the rest of message can be decrypted. Otherwise, the synchronization procedure is repeated using the first block, as described above.

The encryption process of the proposed MKE scheme is illustrated in Fig. 2. The plaintext data blocks (e.g. 128, 156 or 192 bits long) are encrypted with the key chosen by the pseudo-random key selector module. The first encrypted block includes the *key id and random generator's seed* that are necessary to recreate the same key sequence at both transmitter and receiver. Moreover, these values are selected randomly and never transmitted in plain. Hence, the attacker is unable to acquire them.

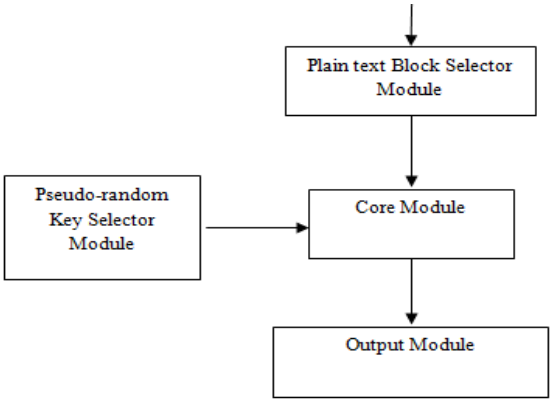

Fig 2. Encryption Module

Decryption process is shown in Fig. 3. Note that an additional processing overhead is introduced when decrypting the first block since the correct key has to be found. Once the first block is decrypted the subsequent blocks are decrypted using keys dictated by the pseudo-random generator. Moreover, in order to minimize the initial overhead, the encoding of the subsequent packets can continue using the same pseudo-random sequence. Then the decoder when using the same sequence will start the key search using the correct one. Hence, no processing overhead will be incurred.

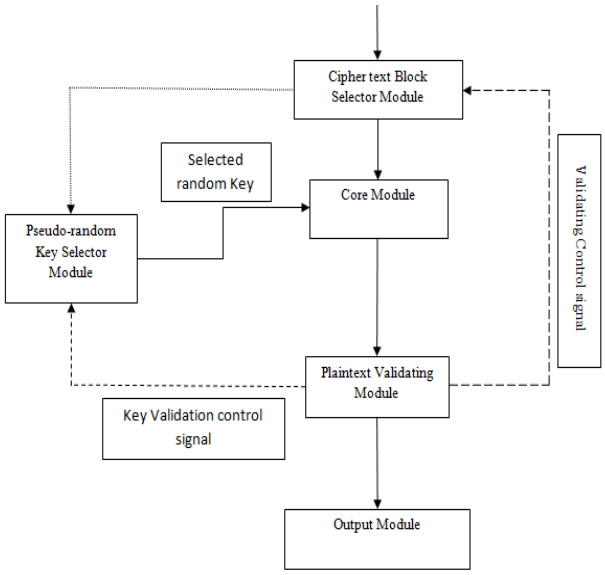

Fig 3. Decryption Module

The existing approaches require significant modification to the encryption engines [17], or use less energy efficient designs [16]. In contrast, the proposed scheme can utilize the S-Boxes with the lowest power consumption that increases energy-efficiency when compared to other schemes [16][17]. Moreover, the security is increased for the same key and cipher size. Next, the analytical and simulation results are presented.

5. THEORETICAL SECURITY ANALYSIS OF THE PROPOSED MKE SCHEME

The security of the proposed multi-key encryption (MKE) scheme is analyzed against the CPA attack and also the brute-force attack. The quantitative results and improvements are presented in next subsections.

A. CPA Attack

Assume that CPA attack on 8 MSBs (Most Significant Bit) of the registers shown in Fig. 4. The key used for this operation is the original key for encryption, *N* random plaintexts and one fixed but random key have been chosen for the experiment, the total number of bit-changes between the previous and the current values of these *M* MSBs of the register for the initial key addition are calculated.

By employing the proposed MKE scheme the correlation between power values with respect to cipher key is broken and correlation coefficients values are reduced. If an attacker employs the CPA method to compromise the secret key, the exact key cannot be decoded since the correlation between the power and the secret key is broken.

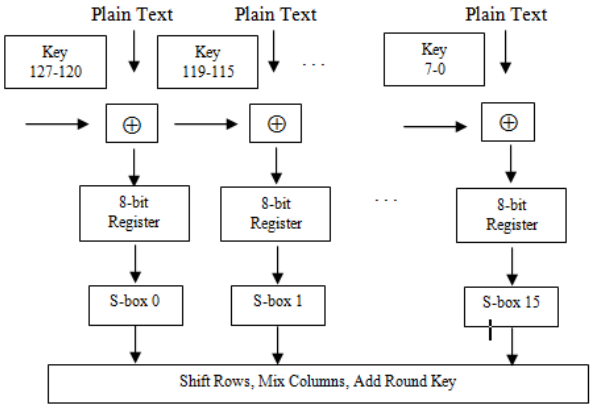

Fig 4. Simplified Diagram of AES Algorithm

Let us consider scenario where two keys are used. Their partial keys are ks1 and ks2 respectively. Then corresponding power values are expressed as

$$P_1 = PT_S \oplus K_{S1} \qquad (6)$$

$$P_2 = PT_S \oplus K_{S2}$$

The correlation can be calculated from (5). When the attacker encrypts N plaintexts, it can calculate correlation between the corresponding power usage for each plaintext and the simulated power consumption of the same plaintexts. The attacker needs to calculate the correlation for every key combination. For a particular key the correlation values are summed up for all plaintexts:

$$\rho_k = \rho_{wp\,1} + \rho_{wp\,2} + ... + \rho_{wpN} \cong N \cdot \rho_{wp} \qquad (7)$$

where p1,p2,…,pN denote the keys used with each plaintexts.

Theorem 1: The correlation factor value decreases with number of employed keys.

Proof: The claim of the Theorem 1 is analyzed for two cases: with two and *M* keys. In short, the combined correlation factor obtained for multiple keys is smaller compared to the correlation factor obtained when employing one key over *N* plaintexts.

Case 1: Encryption using two keys

First, a case with two keys used for encryption is considered. The keys are randomly used to encrypt *N* subsequent message blocks. Let n_{k1} and n_{k2} denotes the number of blocks encrypted with the key *k*1 and *k*2 respectively. Now the correlation factor is equal to

$$\rho_k = n_{K1} \cdot \rho_{wp1} + n_{K2} \cdot \rho_{wp2} = n_{K1} \cdot \rho_{wp1} + (N - n_{K1}) \cdot \rho_{wp2} \qquad (8)$$

where ρ_{wp1} and ρ_{wp2} are the correlation factors corresponding to keys k1 and k2. The difference in correlation factor value due to implementation of multiple keys can be expressed as:

$$\Delta\rho_k = N \cdot \rho_{wp1} - \left[n_{k1} \cdot \rho_{wp1} + (N - n_{k1}) \cdot \rho_{wp2} \right] \qquad (9)$$

where $N > n_{k1}$, and Δρ is the difference between correlation factors when single key and multiple keys are used. If the difference factor is positive, then correlation factors get altered such that exact key used cannot be found. So, using both keys subsequently decreases the overall correlation coefficient value for *N* rounds.

Overall, the following conditions hold: $N > n_{k1}$ and $\rho_{wp1} > \rho_{wp2}$. Consequently, the first difference of correlation factor $\Delta\rho_k$ is always positive which shows that the final correlation values decrease if two keys are used.

Case 2: General formulation for M keys

Following the analysis from the case 1, the correlation factor difference for *M* keys can be expressed as:

$$\Delta\rho_k = N \cdot \rho_{wp1} - \left[n_{k1} \cdot \rho_{wp1} + n_{k2} \cdot \rho_{wp2} + ... + n_{kM} \cdot \rho_{wpM}\right] \quad (10)$$

where $N=\sum_{i=1}^{M} n_{ki}$ and ρ_{wp1} is the highest correlation when compared to the other M-1 keys. Hence, the $\Delta\rho_k$ difference is always positive.

B. Brute Force Attack

The proposed scheme uses random sequence of *N* keys to encrypt block plaintext using AES algorithm. Hence, if *k* keys out of *N* are compromised, the attacker does have to have sufficient information to determine the sequence used to encrypt the message blocks. In this technique the keys are selected randomly and attacker uses every key out of the known *k* keys to decrypt the cipher text for every cipher text block. The number of trials increases with number of blocks in the message and number of known keys, *k*. Moreover, only a fraction of a message is decrypted, as he knows only few out of total number of keys.

In order to find the correct 128-bit key the attacker needs to consider all 2^{128} possible keys. In terms of probability the probability of selecting a correct key is equal to $P = 2^{-128}$. The probability of finding the particular key by brute force, P(T), can be expressed as

$$P(T) = (1-P)^T P \quad (11)$$

Consider an attacker who compromised *k* out of *N* keys. Now, the attacker has to select a key each time from the group of known *k* keys for every cipher text block, and then the probability of selection a key is

$$P(k) = {}^{k}/_{N} \quad (12)$$

Probability of finding exact key from known k keys out of N keys until correct key is found is given as:

$$P_{correct} = (1 - P(k))^{L} \tag{13}$$

where L denotes the number of trials to be performed for each message block to decrypt it until attacker finds the correct key from the known group of keys and it has a maximum value of k (i.e., total number of keys known by the intruder).

The final probability becomes lower than P(T) in (11), where only one key is used. The final probability P_{final}, is the product of P(k) and $P_{correct}$ and is given by

$$P_{final} = P(k) * P_{correct} \tag{14}$$

where P_{final} denotes final probability of finding the correct key for each plaintext block and it denotes increase in security, even if some of the keys out of k keys are compromised attacker has to check each time for the correctness of the key, which results in time consumption as well as only partial detection of the whole message.

The percentage of total message decrypted is proportional to number of k keys known to intruder out of N keys

$$P(percent) \propto k/N \tag{15}$$

The proposed scheme increases the security by using multiple-keys. The security increases proportionally to the number of used keys.

Remark: It has to be noted that the proper design of the random generator (RNG) is required to ensure that attacker cannot finding the order of the keys and thus predict which one is used for each block. A weak RNGs are known to undermine otherwise strong security mechanisms [26] [27].

6. ANALYSIS OF NETWORK RESILIENCE & NETWORK PERFORMANCE FOR MKE SCHEME

The operation of Multi-key scheme [1] in network implementation is similar to q-composite scheme, differing in using the multiple keys for encryption. In q-composite scheme, the multiple shared keys are hashed to obtain an intermediate key which would be used for encrypting the plaintext data. In contrast, the multi-key scheme uses a random key selected out of group of shared keys to encrypt the plaintext data.

In the initialization phase, a set of random keys 'm', will be selected for each node in the network from the total key space S and stored in the node's memory. In the key-setup phase, each node discovers all the common keys with its one-hop neighbors and a simple broadcast message identifies all the keys the node possesses. After key discovery, each node selects a random key from the group of shared keys and considers a random key for every plaintext block. Synchronization is very essential for successful encryption and decryption of the encrypted messages.

Here the multi-key scheme is evaluated in terms of network connectivity and resilience against node capture.

A. Network Connectivity:

It is assumed that the connectivity of the network depends on parameters

- Number of nodes in the network is an important factor in determining the connectivity of the network. The density of nodes in the network impacts the connectivity because the more number of nodes in a fixed area the more probability of nodes sharing common keys to communicate with the destination nodes.
- Number of keys in the key pool 'S' is one of the important factor in determining the connectivity of the network. It is an important factor because the more the key pool size the better the security against node capture but the lesser the probability of nodes sharing common shared keys. So it is important to maintain a tradeoff between security and the connectivity of the network.
- Number of keys stored per node is one of the factors which impact the connectivity. The more number of keys stored in nodes will help in improving the

connectivity of the network but it weakens the nodes' resilience to node capture. Additionally, it impacts the memory cost incurred per node

- Number of keys required for communication is vital parameter in determining the connectivity as well as resilience against node capture. The requirement of more number of keys for communication compel the nodes to store more number of keys per node or reduce the key pool size for better connectivity.

B. Resilience Against Node Capture:

In the existing schemes, network's resilience is calculated by the fraction of links in the network that an attacker able to eavesdrop from the result of recovering keys from captured nodes. In MKE implementation, consider the resilience offered by MKE scheme, the resilience is assumed as combination of resistance offered in compromising nodes (against CPA attack) and resistance offered to attacker in eavesdropping on additional nodes to capture keys.

Here we initially discuss the resilience towards node capture to compromise the keys.

Theorem 2:

The network's resilience against node capture increases with the MKE scheme

Proof: The claim of theorem 2 is to state that the resistance to node compromise is more prominent due to MKE scheme rather than with single key scenario.

The correlation factor for each guessed key shown in fig 11 follows either a positive or negative exponential distribution over 'N' plaintexts. However, the exponential distribution rate is not at constant rate but varies with the parameter 'λ'; which is correlation between power consumption and bit values varied in a register.

So, the distribution followed by correlation factor for each guessed key is given by

$\rho_k(t) = \lambda . e^{\lambda t}$, where

$$\lambda = \frac{E(H(\rho)W) \quad E(H(\rho))E(W)}{\sigma(H(\rho))\sigma(W)}$$

$$\rho_{k(t)} = \lambda_1 . e^{\lambda_1 t_1} + \lambda_2 . e^{\lambda_2 t_2} + \ldots\ldots\ldots\ldots\ldots + \lambda_n . e^{\lambda_n t_n}$$

At every particular time instant or for each plaintext, 'λ' parameter varies which has been expressed above. In normal AES implementation 'λ' parameter is proportional to single key's hamming distance

$\lambda \alpha H(P_s \oplus K, P_s \oplus K)$

$\lambda \alpha H(K, K)$

Here H () is hamming distance model defined in eqn (2)

$\rho_{k(t)= \lambda_1 . e^{\lambda_1 t_1} + \lambda_2 . e^{\lambda_2 t_2} + \ldots\ldots\ldots\ldots\ldots + \lambda_n . e^{\lambda_n t_n}}$

$\lambda \alpha H(P_s \oplus K_{s,} P_s \oplus K_n)$ n=1,2,…m where 'm' is number

$$\lambda \alpha \begin{cases} H(P_s \oplus K_{s,} P_s \oplus K_1) - \ if \ k_1 \\ H(P_s \oplus K_{s,} P_s \oplus K_2) - \ if \ k_2 \end{cases}$$

'λ' parameter varies for various plaintexts within in a maximum threshold value of Δλ

For AES implementation,

$\lambda = E(\lambda) \pm \Delta\lambda \, , \lambda \alpha H(k, p_i)$

$\rho_{k_1}(t_1) = \sum_{i=1}^{N} (E(\lambda_1) + \Delta\lambda_1) \, . \, e^{(E(\lambda_1) + \Delta\lambda_1)}$

For MKE scheme,

$\lambda = E(\lambda) \pm \lambda_n \Rightarrow \quad E(\lambda) \pm \Delta\lambda_1, \Delta_{\lambda_n} \alpha H(K_{s,}, K_n)$

$E(\lambda) \pm \Delta\lambda_2$

$E(\lambda) \pm \Delta\lambda_n$

$\rho_{k_1 k_2}(t_1) = \sum_{i=1}^{P.N} (E(\lambda_1) + \Delta\lambda_1) \, . \, e^{(E(\lambda_1) + \Delta\lambda_1)} + \sum_{i=1}^{(N - P.N)} (E(\lambda_2) + \Delta\lambda_2) \, . \, e^{(E(\lambda_2) + \Delta\lambda_2)}$

To generalize:

$\rho_{k_1} = \sum_{i=1}^{N/2} (E(\lambda_1) + \Delta\lambda_1) \, . \, e^{(E(\lambda_1) + \Delta\lambda_1)} + \sum_{i=1}^{N/2} (E(\lambda_1) + \Delta\lambda_1) \, . \, e^{(E(\lambda_1) + \Delta\lambda_1)}$

$\rho_{k_1 k_2} = \sum_{i=1}^{N/2} (E(\lambda_1) + \Delta\lambda_1) \, . \, e^{(E(\lambda_1) + \Delta\lambda_1)} + \sum_{i=1}^{N/2} (E(\lambda_2) + \Delta\lambda_2) \, . \, e^{(E(\lambda_2) + \Delta\lambda_2)}$

$\rho_{kn} = \sum_n \sum_{i=1}^{z} (E(\lambda_1) + \Delta\lambda_1) . \, e^{(E(\lambda_1) + \Delta\lambda_1)}$ (16)

The difference in correlation values between both the implementations should be negative

$(\rho_{k_1 k_2} - \rho_{k_1}) = (\sum_{i=1}^{N/2} (E(\lambda_1) + \Delta\lambda_1) \, . \, e^{(E(\lambda_1) + \Delta\lambda_1)} + \sum_{i=1}^{N/2} (E(\lambda_2) + \Delta\lambda_2) \, . \, e^{(E(\lambda_2) + \Delta\lambda_2)})$

$- \ (\sum_{i=1}^{N/2} (E(\lambda_1) + \Delta\lambda_1) \, . \, e^{(E(\lambda_1) + \Delta\lambda_1)} + \sum_{i=1}^{N/2} (E(\lambda_1) + \Delta\lambda_1) \, . \, e^{(E(\lambda_1) + \Delta\lambda_1)} \ )$

$(\rho_{k_1 k_2} - \rho_{k_1}) = (\sum_{i=1}^{N/2} (E(\lambda_2) + \Delta\lambda_2) \, . \, e^{(E(\lambda_2) + \Delta\lambda_2)} - \sum_{i=1}^{N/2} (E(\lambda_1) + \Delta\lambda_1) \, . \, e^{(E(\lambda_1) + \Delta\lambda_1)} \ )$

$(\rho_{k_1k_2} - \rho_{k_1}) = (\sum_{i=1}^{N/2}(E(\lambda_2).\ e^{(E(\lambda_2)+\Delta\lambda_2)} - E(\lambda_1)e^{(E(\lambda_1)+\Delta\lambda_1)}) + (\sum_{i=1}^{N/2}(\Delta\lambda_2 .\ e^{(E(\lambda_2)+\Delta\lambda_2)} - \Delta\lambda_1.e^{(E(\lambda_1)+\Delta\lambda_1)}))$

Since λ is proportional to hamming distance with respect to secret key used for encryption, each of the correlation values can be defined in terms of hamming distance values.

$\lambda_1=\lambda_2 + a.D \Rightarrow \lambda_2 = \lambda_1 - a.D$

$$(\rho_{k_1k_2} - \rho_{k_1}) = \left[\sum_{i=1}^{\frac{N}{2}}\left[E(\lambda_1 - a.D).e^{(E(\lambda_1 - a.D)+\Delta\lambda_2)} - E(\lambda_1).e^{(E(\lambda_1)+\Delta\lambda_1)}\right]\right]$$

$$+\left[\sum_{i=1}^{\frac{N}{2}}\left[(\Delta\lambda_1 - a.D).e^{(E(\lambda_1)+\Delta\lambda_2.a.D)} - \Delta\lambda_1.e^{(E(\lambda_1)+\Delta\lambda_1)}\right]\right]$$

$$[\because \Delta\lambda_2 = \Delta\lambda_1 - a.D, \Delta\lambda_2 - a.D = \Delta\lambda_1 - 2(a.D)]$$

$$(\rho_{k_1k_2} - \rho_{k_1}) = \left[\sum_{i=1}^{\frac{N}{2}}\left[E(\lambda_1).e^{E(\lambda_1)+\Delta\lambda_1}.\left[\frac{1}{e^{2.(a.D)}} - 1\right] - a.D.\frac{e^{E(\lambda_1)+\Delta\lambda_1}}{e^{2.(a.b)}}\right]\right]$$

$$+\left[\sum_{i=1}^{N/2}\left[\Delta\lambda_1 .e^{(E(\lambda_1)+\Delta\lambda_1)}\left[\frac{1}{e^{2.(a.D)}} - 1\right] - a.D\ \frac{e^{(E(\lambda_1)+\Delta\lambda_1)}}{e^{2.(a.D)}}\right]\right]$$

$$(\rho_{k_1k_2} - \rho_{k_1}) = \left[\frac{1}{e^{2(a.D)}} - 1\right]\left[\sum_{i=1}^{N/2}\left[(E(\lambda_1) + \Delta\lambda_1).e^{E(\lambda_1)+\Delta\lambda_1}\right]\right] - \frac{2.a.D.e^{E(\lambda_1)+\Delta\lambda_1}}{e^{2(a.D)}} < 0$$

The above equation defines the difference in correlation values between both the implementations is definitely negative.

The probability of determining the guessed key to be exact secret key used for encryption is given by

$$p_1 = \frac{\rho_{kn}.(p)}{\rho}$$

$$p_1 = \frac{\sum n \sum_{i=1}^{z}(E(\lambda_1)+\Delta\lambda_1).e^{(E(\lambda_1)+\Delta\lambda_1)}.(p)}{\rho_{k1}} \quad (17)$$

To find the number of plaintexts required to achieve the desired level of correlation factor (attacker defines certain threshold) is given by

$$N_k = \frac{\rho_{kn.(N)}}{\rho} \quad (18)$$

Here ‘N’ is number of plaintexts assumed for AES implementation to achieve the threshold level.

The resilience against node capture is calculated as product of probabilities in capturing initial set of nodes and compromising additional set of communication links.

If ‘x’ nodes are captured and ‘m’ keys are revealed then the probability that a certain key not being compromised is a conditional probability between eqn (17) and the following probability

P = (1- $\frac{m}{s}$)(1- $\frac{m}{s}$)…… x times

P = $(1-\frac{m}{s})^{x}$ (fraction of keys not compromised)

Total fraction of keys that have been compromised is given by

F = $\left[1-(1-\frac{m}{s})^{x}\right]$

In MKE scheme, multiple keys are used for encryption. So, to compromise a secure link the probability is

F = $\left[\left[1-(1-\frac{m}{s})^{x}\right]\right]^{i}$

The probability of setting up a secure link is

P = P(q)+P(q+1)……P(m)

$P_2 = \sum_{i=q}^{m} F.\frac{P(i)}{P}$

$P_2 = \sum_{i=q}^{m}(1-(1-\frac{m}{s})^{x})^{i}.\frac{P(i)}{P}$, (19)

where P (i) = $\frac{\binom{s}{i}\binom{s-i}{2(m-1)}\binom{2(m-1)}{(m-1)}}{\binom{s}{m}^{2}}$

In the above equation, p(i) defines the probability of two nodes sharing ‘i’ keys

So, the resilience against node capture is given by the probability p_{final}

$p_{final} = p_1.p_2$

$p_{final} = \left(\frac{\sum_n \sum_{i=1}^{z}(\mathrm{E}(\lambda_1)+\Delta\lambda_1).e^{(\mathrm{E}(\lambda_1)+\Delta\lambda_1).(p)}}{\rho_{k1}}\right).p_2$ (20)

7. SIMULATION RESULTS

Simulation has been conducted in Matlab to analyze the performance of the proposed MKE schemes in thwarting the CPA attack. Attack on a partial 8-bit key is studied. However, the results can be easily expanded to the general case of *L*-bit key. The results are presented based on reference to the respective keys. The key with highest correlation is expected to be the secret key used for the actual encryption. The proposed technique uses multiple keys subsequently for *N* plaintexts, which results in the reduced correlation.

In CPA attack, the complexity of attack increases with number of plaintexts, N. Also, the confidence of finding the correct key increases with number of plaintexts, N, since the individual correlation coefficients of *N* plaintexts are being summed up. However, the confidence saturates at some level due to noise in measurements and quality of the power correlation for the given circuitry. Furthermore, in case of the MKE scheme, the signal correlation reduces when compared to a single key scheme since the random selection of keys breaks the correlation between power consumption and the key. This tradeoff between increasing complexity and saturating confidence leads to a practically justifiable size of the plaintext set, N. Henceforth, the N=1000 value is typically considered for this experiment[16][17].

Fig. 5 illustrates the raw correlation factors for a single key scenario [17]. It exhibits a high correlation with the secret key that was used during the actual encryption. In contrast, for MKE scheme the correlation between secret key and correlation coefficients decrease with number of used keys, as shown in Fig 6. The main reason is that the subsequent blocks are encrypted with different keys, which power correlation with the simulated results for single key decreases.

For the two key case, as shown in Fig. 6, the highest correlation occurs for *I*=256. This is different from single-key case presented in Fig. 7 since the MKE technique randomly select keys that reduces overall correlation factor averaged over *N* blocks of data.

In this case, two keys are randomly chosen to encrypt *N*=1000 plaintexts or blocks of data. Assuming that attacker have no idea of MKE scheme, correlates *N***g* cases (*g*=256) for each of the *g* keys with power consumption values of *N*=1000 plaintexts (uses two keys for encryption).

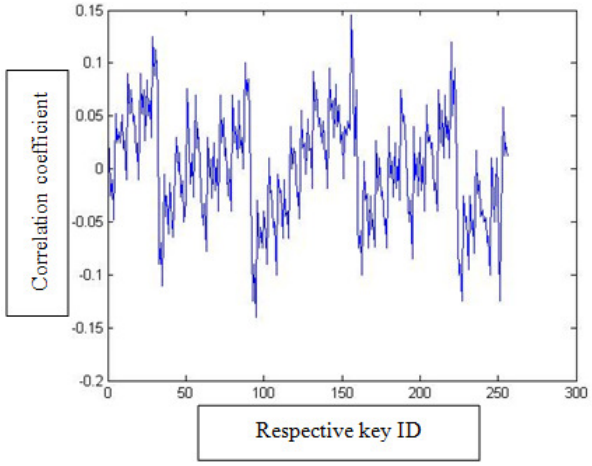

Fig 5. Correlation Coefficients for Single Key Usage [17]

It results in lower correlation values with only one of the key among the two having the highest correlation (one key match with original key in ‘g’ keys and other key negating). Moreover, the equation (10) can be interpreted as an average of the correlations of the used keys.

Hence, the overall correlation reduces with the number of used keys since the average over the whole domain space is equal to zero. Next, the proposed scheme is analyzed from energy-efficiency point of view.

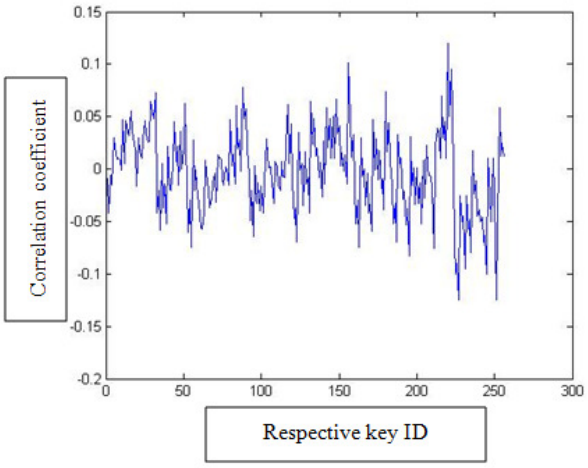

Figure 6. Correlation Coefficients for Two Keys Usage

Energy Efficiency Analysis

The energy efficiency is measured as the energy consumed by encryption engine to transmit a given message. The analysis assumes the AES-based engine that operates on 128-bit blocks (128-bit key size). In general, the AES algorithm can be implemented using various S-Box designs, for example LUT, SOP, etc. These S-boxes have different energy efficiency and power correlation. In the scheme proposed in [17] the authors utilize a combination of several different designs in order to reduce power correlation. However, the power consumption increases since the scheme uses S-boxes with a high-energy consumption.

In contrast, the proposed MKE scheme improves the energy-efficiency compared to the technique in [17] since it can employ the S-box design with lowest power consumption, as shown in Fig. 7. The comparison between power consumption of the technique in [17] and the proposed scheme illustrates that even with the initial synchronization overhead (i.e. finding the first key in sequence) the proposed scheme outperforms the other scheme. Moreover, the proposed scheme scales better with size of the message since it allows using the S-boxes with the lowest power footprint.

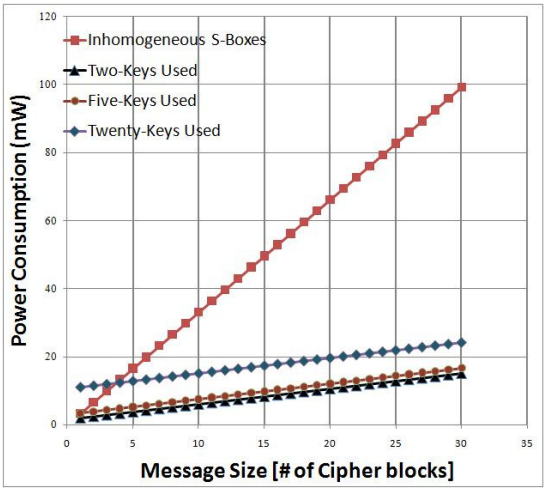

Figure 7. Comparison of Power Consumption for Multi-Key Encryption (MKE) Scheme

The effect of the network evaluation parameters discussed in section VI is simulated using Ns2 tool and compared based on contributing factors described below.

Here,

T1 = Number of keys in key pool

T2 = Number of keys per node

T3 = Number of nodes in the network

T4 = Number of keys required for communication

Fig 8 shows the impact of the density of nodes on the connectivity factor. In general, the network connectivity improves with increasing density as shown for all cases in Fig. 8. A better connectivity can be achieved for less denser network if the size of key pool 'S' is small or number of keys per node is increased provided nodes are not far apart.

Distance between nodes is an alternative term for the density of nodes in network. Since nodes are randomly deployed it is essential that a careful approach is needed in defining other network selection parameters. From the Fig. 8 it can be stated that the increase in key pool size reduces network connectivity and it can be improved by increasing the number of keys stored per node.

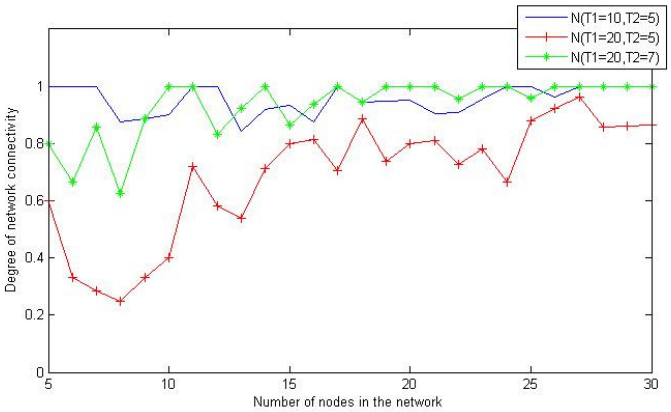

Figure 8. Network Connectivity Vs. Number of Nodes in the Network

Fig. 9 shows how the connectivity could be varied with number of keys in key pool 'S' and increase in key pool size for a specified configuration decreases the connectivity for the network. So to improve the connectivity we can increase the number of keys stored per node such that more common keys can be shared among the nodes. From the Fig. 9, the increase in requirement to have more keys for communication, there is reduction in network connectivity and to improve the performance of the network in terms of connectivity the number of keys stored per node can be increased.

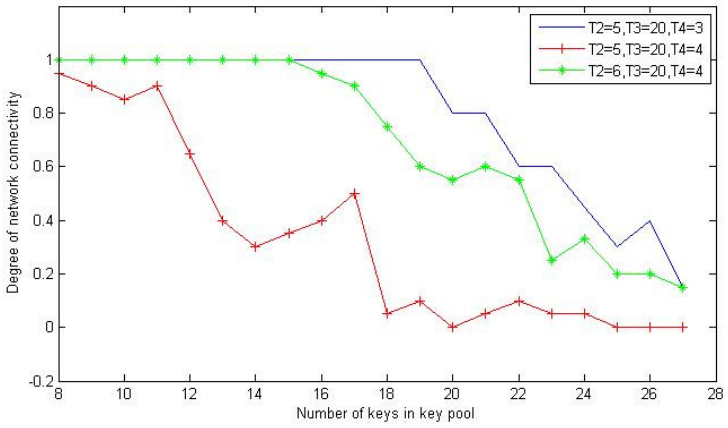

Figure 9. Network Connectivity Vs. Number of Keys in the Key Pool

Fig 10 shows how connectivity varies with number of keys stored per node. As from the graph, better connectivity can be achieved if key pool size 'S' is reduced with fixed number of keys per node. From the Fig. 10, better connectivity can be achieved by storing more number of keys per node or reducing number of keys required for communication.

Fig 11 shows how the network connectivity varies with number of keys required for communication. Two nodes in the network can communicate using MKE scheme only if the required number of multiple keys are available for encryption. If the keys required for communication is high then achieving higher network connectivity is a difficult task.

From the Fig. 11, to improve the connectivity with higher communication key requirements the network can be made denser which will slightly improve the connectivity. Network connectivity can be improved by reducing the key pool size such that there is more probability of nodes sharing common keys for communication.

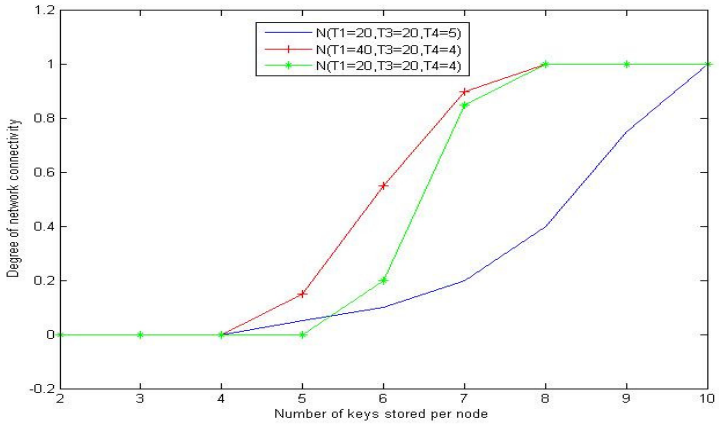

Figure 10. Network Connectivity Vs. Number of Keys Stored Per Node

Hence to design a network it is essential to consider each of the discussed parameter for any management scheme for better connectivity. From the simulation results, a table is constructed for better connectivity results with respect to different network configurations.

Energy consumption model is simulated in NS2 with network of 30 nodes and compared with typical AES implementation. AODV routing protocol is considered as routing protocol in the implementation.

When a node intends to send a message it encrypts the message with additional data fields shown in Fig. 1. The receiving node tries to decrypt with each of the key in its memory and checks to match with the key ID. In further encounters, node decrypts subsequent messages based on the seed value to accurately predict the matching key for decryption.

For the energy model simulation, the transmitting, receiving and idling powers are assumed to be 0.65W, 0.395W and 0.035W. The total energy consumed in the network is calculated and simulated for both the AES and MKE implementations. MKE scheme initially consumes more energy which can be referred from Fig. 12 because of more computation involved per node for matching key ID purposes. However, MKE scheme uses low energy S-Boxes in its architecture design which makes the energy consumed factor slowly approaching AES scheme with time.

Table 1 presents comparison for different network scenarios. The final energy consumption values are tabulated for both the AES and MKE implementations. The MKE implementation uses low-energy S-Boxes which reduce energy consumption and so MKE implementation is better to be employed.

Fig. 13 illustrates the network's resilience in terms of fraction of communication links compromised based on the number of captured nodes. From the Fig. 13 the MKE scheme has better resilience when compared with single key implementation scheme. A better resilience is observed with the usage of multi-key scheme (5 keys) from the Fig. 13 because only a fraction of link security is compromised in the case of capturing a node.

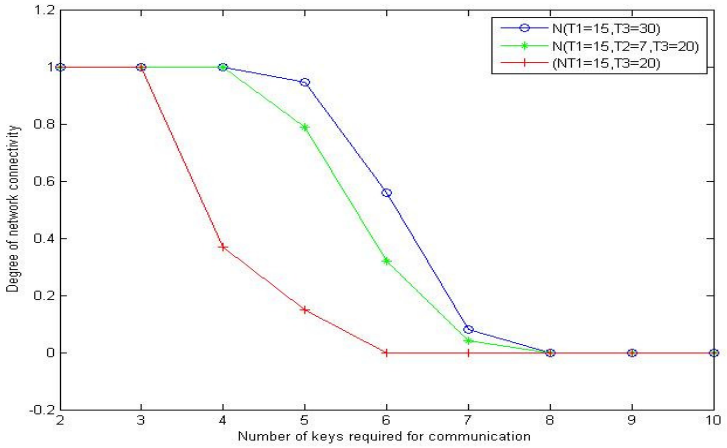

Figure 11. Network Connectivity Vs. Number of Keys Required for Communication

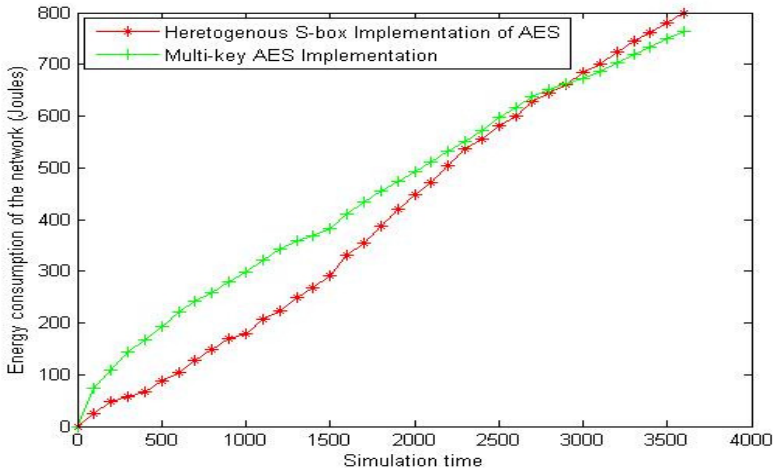

Figure 12. Comparison of Energy Model between AES and MKE Schemes

Additionally, in the case of MKE scheme the resilience is calculated as product of probabilities in capturing initial set of nodes and compromising additional set of communication links. It is outperformed by other implementations after certain period where much of the network is compromised and because of holding multiple keys for communication most of the keys are revealed to the attacker.

Table 1. Energy Consumption for Various Configurations

Network Configuration	AES Implementation (Joules)	MKE Implementation (Joules)
T2=5, T3=30	636.23J	596.36J
T2=7, T3=40	848.62J	797.73J
T2=4,T3=20	424.31J	402.12J

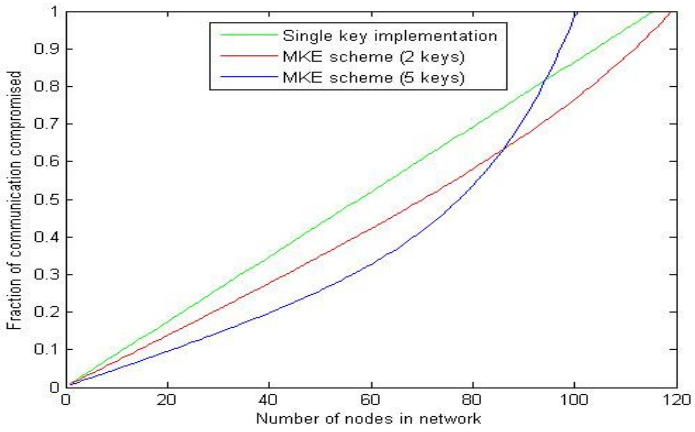

Figure 13. Fraction of the Network Communication Compromised Vs. Captured Nodes in the Network

However, it has to be noted that there is stiff resistance to attacker to compromise initial set of nodes for MKE scheme (5 keys) scenario which is the essential criterion of any security algorithm. Above 85% of nodes being compromised the security for MKE quickly deteriorates since it becomes difficult to find sufficient number of nodes with shared keys. However at this point almost entire network is compromised regardless of security scheme employed.

8. CONCLUSION

The proposed MKE technique has been shown to improve the security of AES algorithm against CPA attack while minimizing power consumption. Additionally, it improves security of AES against brute-force attacks.

In the case of a CPA attack, the MKE scheme thwarts a CPA type attack by reducing correlation between power consumption and the key. The proposed scheme, using 5 keys can decrease the correlation by 80% between power and data. Also, the energy consumption of the proposed MKE scheme reduces by over 70% when compared to the inhomogeneous S-boxes scheme while maintaining high security. Additionally, single key compromises only a small fraction of the message thus increasing security against brute-force attacks. Consequently, all the keys have to be compromised before the link becomes unsecure.

MKE scheme when implemented in network implementation is able to improve the resilience of the network against node capture compared to existing schemes. MKE scheme is analyzed analytically such that time to compromise or number of plaintexts required to achieve confidence level of the attacker can be found. This enables the user to periodically update the keys such that nodes can be secured from the attacks.MKE scheme is also able to improve energy efficiency of the network compared to existing schemes which makes the network to sustain for longer life periods.

9. REFERENCES

[1] Sandeep Kolli, Maciej Zawodniok, "Energy-efficient multi-key security scheme for wireless sensor networks", 5th LCN workshop on Security in Communication Networks, Zurich, Switzerland. Proceedings of 34th IEEE LCN, 21-23 Oct 2009.

[2] Gupta, A, Kuri. J, "Deterministic schemes for key distribution in wireless sensor networks", Communication Systems Software and Middleware and Workshops, 2008. COMSWARE 2008, 3rd International Conference, 6-10 Jan. 2008.

[3] Park, E. C. Blake, I.F, "Reducing Communication Overhead of Key Distribution Schemes for Wireless Sensor Networks", Computer Communications and Networks, 2007. ICCCN 2007. Proceedings of 16th International Conference, 13-16 Aug 2007.

[4] L. Eschenauer and V. D. Gligor, "A key management scheme for distributed sensor networks," in Proceedings of the 9th ACM Conference on Computer and Communication Security (CCS '02), pp 41–47, Washingtion, DC, USA, November 2002.

[5] H. Chan, A. Perrig, and D. Song, "Randomkey predistribution schemes for sensor networks," in Proceedings of IEEE Symposium on Security and Privacy, pp 197–213, Oakland, Calif, USA, May 2003.

[6] W. Du, J. Deng, Y. S. Han, P. Varshney, J. Katz, and A. Khalili, "A pairwise key predistribution scheme for wireless sensor networks," ACM Transactions on Information and System Security, vol. 8, no. 2, pp 228–258, 2005.

[7] Liu, P. Ning, and R. Li, "Establishing pairwise keys in distributed sensor networks," ACM Transactions on Information and System Security, vol. 8, no. 1, pp 41–77, 2005.

[8] R. Blom, "An optimal class of symmetric key generation systems," in Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques (EUROCRYPT '84), pp 335–338, Paris, France, April 1985.

[9] Zhihong Liu, Jianfeng Ma, Qiping Huang and sangjae moon, " A pairwise key Establishment scheme for Heterogeneous sensor networks", 2008 ACM(Hetersanet08, may 30,2008, Hong Kong SAR,china).

[10] Sajid Hussain, Firdous Kausar and Ashraf Masood, "An Efficient key distribution scheme for Heterogeneous sensor networks" 2007 ACM (IWCMC'07, August 12-16,2007,Hawaii,USA).

[11] S. Basagni, K. Herrin, D. Bruschi and E. Rosti, Secure pebblenets, in Proceedings of the 2001 ACM International Symposium on Mobile ad hoc networking & computing, Long Beach, CA, USA (2001) pp 156–163. ACM Press.

[12] R. Di Pietro, L.V. Mancini and S. Jajodia, Providing secrecy in key management protocols for large wireless sensors networks, Journal of AdHoc Networks, 1(4) (2003) pp 455–468.

[13] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis", Advances in Cryptology - Crypto 1999, LNCS 1666, pp 388-397, Springer-Verlag, 1999.

[14] Siddika Berna Örs, Frank K. Gurkaynak, Elisabeth Oswald, and Bart Preneel. "Power-Analysis Attack on an ASIC AES Implementation", In Proceedings International Conference on Information Technology-ITCC 2004, Las Vegas, USA.

[15] Norbert Pramstaller, Elisabeth Oswald, Stefan Mangard, et al., "A Masked AES ASIC Implementation", in Proceedings of Austrochip 2004, Villach, Austria, Oct. 8, 2004.

[16] Zheng Zhoxia, Zou Xuecheng, Liu Zhenglin, Chen Yicheng "Secure AES Coprocessor against Power Analysis for Wireless Sensor Networks", Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference, sept 2007 IEEE.

[17] Zheng Zhoxia, Zou Xuecheng, Liu Zhenglin, Chen Yicheng "Security Analysis and Optimization of AES S-boxes Against CPA attack in Wireless Sensor Network" , Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference, sept 2007 IEEE.

[18] Advanced Encryption Standard (AES)", Federal Information Processing Standards Publication 197, Nov. 2001.

[19] D. Coppersmith, D. B. Johnson and S. M. Matyas, "A Proposed mode for triple-DES encryption", IBM J.RES Develop. Vol 40, No.2, March 1996.

[20] Haowen Chan, Adrian Perrig and Dawn Song, "Random Key Pre-distribution Schemes for Sensor Networks", IEEE Symposium on Security and Privacy, pp 197-213, 2003.

[21] Ting Yuan, Jianquing Ma and Shiyong Zhang, "Random key Management using group deployment in large-scale sensor networks", Third International conference on Communications and Networking in China, Chinacom 2008, pp 1167-1171, pp 25-27, Aug 2008.

[22] Kevin Chan and Faramarz Fekri, "A Resiliency-Connectivity metric in wireless sensor networks with key predistribution schemes and node compromise attacks", Physical Communication, Vol1, Issue 2, pp 134-145, Elsevier, June 2008.

[23] Zhong Su, Chuang Lin, Fengyuan Ren, Yixin Jiang, and Xiaowen Chu, "An Efficient Scheme for Secure Communication in Large-scale Wireless Sensor Networks", IEEE, 2009.

[24] Sujun Li, Qiaoliang Li, Boqing Zhou, "A New Efficient Pairwise Key Establishment Scheme for Wireless Sensor Networks", IEEE, 2007.

[25] Dijiang Huang, Deep Medhi, "A Byzantine Resilient Multi-path Key Establishment Scheme and Its Robustness Analysis for Sensor Networks", Proceedings of 19th IEEE International Parallel and Distributed Processing Symposium, IEEE, 2005.

[26] IBM 1961 BRL Report.

[27] Halfill, Tom R. (2006-10-10). "204101.qxd Ambric's New Parallel Processor". Microprocessor Report (Reed Electronics Group): 1–9.

[28] S. Guilley, P. Hoogvorst, R. Pacalet, "Differential Power Analysis Model and some Results", In proceedings of CARDIS 2004, Kluwer Academic Publishers, pp 127-142, 2004.

[29] John Kelsey, Bruce Schneier, David Wagner, and Chris Hall S. Vaudenay, "Cryptanalytic attacks on Pseudorandom key generators", FSE'98, LNCS 1372, pp 168{188}, Springer-Verlag Berlin Heidelberg 1998.

[30] M. Dichtl, "How to Predict the Output of a Hardware Random Number Generator", Proceedings of the Workshop on Cryptographic Hardwareand Embedded Systems – CHES 2003, LNCS 2779, pp 181–188, Springer-Verlag Berlin Heidelberg.

2. CONCLUSION AND FUTURE WORK

This work proposes DP based communication model which incorporates MKE scheme for security purpose improves the performance of wireless networks. It has reduced the energy consumption costs for the data transmission as well as processing cost by 65% and practically doubled the network lifetime. Also, it reduced the energy inequalities among the network thus improving utilization of the network resources.

Additionally, the communication cost in terms of delay is reduced since fewer bits have been transmitted. Consequently, the communication bottlenecks have lesser effect on the quality of service. The proposed scheme incorporates MKE security scheme that reduces the overhead caused due to security implementation in terms of energy consumed and process delay, which are often neglected in existing security implementations for wireless networks.

This work proposes MKE scheme by improving the way the AES algorithm is utilized on links. As a result the MKE improved resilience against a CPA attack while minimizing power consumption. Additionally, it also improves security of AES against brute-force attacks.

MKE scheme thwarts CPA attack by reducing correlation between power consumption and the key. The proposed scheme, using 5 keys can decrease the correlation by 80% between power and data. Also, the energy consumption of the proposed MKE scheme reduces by over 70% when compared to the inhomogeneous S-boxes scheme while maintaining high security. Discussed at network level, compromising single key would only compromise a fraction of message thus increasing security against brute-force attacks. Consequently, all the keys have to be compromised before the link becomes unsecure.

MKE scheme in network implementation is able to improve resilience of the network against node capture compared to existing schemes. MKE scheme is analyzed analytically such that time to compromise or number of plaintexts required to achieve confidence level of the attacker can be found. This enables the user to periodically update the keys such that nodes can be secured from the attacks. It is also able to improve energy efficiency of the network compared to existing schemes, which makes the network to

sustain for longer life periods. Hence the proposed work improves the energy efficiency and performance of the wireless networks while ensuring high data security.

APPENDIX

Table 1. Cost and time estimation for a brute force attack

Machine cost	Key Search Time in 2009	Key Search Time in 1995
$300M	9.37×10^{15} years	4.52×10^{23} years
$300K	6.52×10^{24} years	5.6×10^{33} years
$10K	7.42×10^{36} years	Infeasible

Table 2. Hardware cost of processing power

Corresponding year	Hardware cost/1000MIPS
1961	$1.1 trillion
1997	$30,000
2007	$0.42

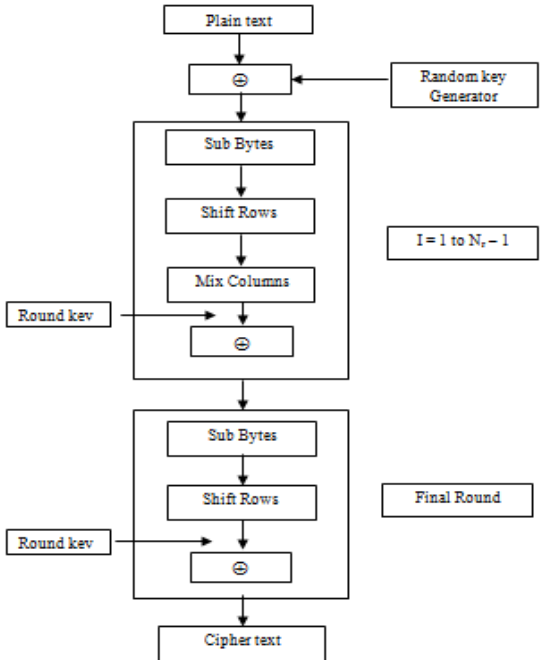

Fig 1. Modified Architecture for AES Encryption Algorithm

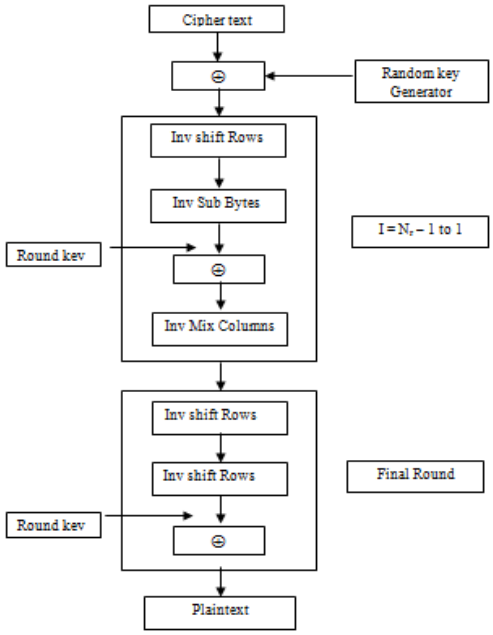

Fig 2. Modified Architecture for AES Encryption

BIBLOGRAPHY

[1]A. Manjeshwar and D.P. Agarwal, "TEEN: A routing protocol for enhanced efficiency in wireless sensor networks," Proc. Of 15th parallel and Distributed processing symposium, 2001.

[2]A. E. Gamal, C. Nair, B. Prabhakar and S. Zahedi, "Energy-efficient scheduling of packet transmissions over wireless networks", IEEE Infocom, 2002.

[3]D. P. Bertsekas, Dynamic Programming: Deterministic and Stochastic Models. Prentice-Hall, Inc., Englewood Cliffs, 1987.

[4]A. Ciancio and A. Ortega, "A Dynamic Programming Approach to Distortion-Energy Optimization for Distributed Wavelet Compression with Applications to Data Gathering In wireless Sensor Networks," Proc of 2006 IEEE International conference on Acoustics, Speech and Signal processing, May 2006, pp 14-19.

[5]W. G. Yang, T. D. Guo and T. Zhao, "Routing algorithms of the wireless sensor network based on dynamic programming", in Journal of Computer Research and Development, 2007, pp 890-897.

[6]Gyouhwan Kim and Rohit Negi, "Dynamic programming for scheduling a single route in wireless networks", IEEE 2007.

[7]Lingyang Song , Yan Zhang , Rong Yu , Wenqing Yao , and Zhuo Wu, "Cross-layered Optimized Routing for Wireless Sensor Networks Using Dynamic Programming", IEEE, 2009.

[8]Sandeep kolli, Maciej Zawodniok, "Energy-efficient multi-key security scheme for wireless sensor networks", 5th LCN workshop on Security in Communication Networks, Zurich, Switzerland. Proceedings of 34th IEEE LCN, 21-23 Oct 2009.

[9]P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis", Advances in Cryptology -Crypto 1999, LNCS 1666, pp 388-397, Springer-Verlag, 1999.

[10]Siddika Berna Örs, Frank K. Gurkaynak, Elisabeth Oswald, and Bart Preneel. "Power-Analysis Attack on an ASIC AES Implementation", In Proceedings International Conference on Information Technology-ITCC 2004, Las Vegas, USA, Proceedings, 2004.

[11] S. Basagni, K. Herrin, D. Bruschi and E. Rosti, Secure pebblenets, in Proceedings of the 2001 ACM International Symposium on Mobile ad hoc networking & computing, Long Beach, CA, USA (2001) pp 156–163. ACM Press.

[12] H. Chan, A. Perrig, and D. Song, "Randomkey predistribution schemes for sensor networks," in Proceedings of IEEE Symposium on Security and Privacy, pp. 197–213, Oakland, Calif, USA, May 2003.

[13]W. Du, J. Deng, Y. S. Han, P. Varshney, J. Katz, and A. Khalili, "A pairwise key predistribution scheme for wireless sensor networks," ACM Transactions on Information and System Security, vol. 8, no. 2, pp 228–258, 2005.

[14]D. Liu, P. Ning, and R. Li, "Establishing pairwise keys in distributed sensor networks," ACM Transactions on Information and System Security, vol. 8, no. 1, pp 41–77, 2005.

[15]Advanced Encryption Standard (AES)", Federal Information Processing Standards Publication 197, Nov. 2001.

[16]Haowen Chan, Adrian Perrig and Dawn Song, "Random Key Predistribution Schemes for Sensor Networks", IEEE Symposium on Security and Privacy, pp 197-213, 2003.

[17]Ting Yuan, Jianquing Ma and Shiyong Zhang, "Random key Management using group deployment in large-scale sensor networks", Third International conference on Communications and Networking in China, Chinacom 2008, pp 1167-1171, 25-27 Aug 2008.

VITA

Sandeep Chowdary Kolli was born on August 5, 1986 in Repalle, Andhra Pradesh, India. Sandeep received his school education from Vishwavani public school, Vijayawada, India. He received his intermediate education from Gowtham Junior College, Gudavally, India. He completed his Bachelor of Technology (B.Tech) in Electronics and Communication Engineering from Jawaharlal Nehru Technological University, Hyderabad, India in May 2007. He worked as Program Engineer in Wipro Technologies, Bangalore, India from June 2007 - July 2008. He started his Master of Science program in Electrical and Computer Engineering at Missouri University of Science and Technology in August 2008. He graduated in June 2010. He is a member of IEEE.