Network and Complex Systems
ISSN 2224-610X (Paper) ISSN 2225-0603 (Online)
Vol.4, No.4, 2014

www.iiste.org

Anlytical study based on issues of Routing & Security in Wireless sensor networks

Ashish Bagwari
Assistant Professor, UTU, Uttarakhand, INDIA

Menka Goswami
Dept. of CSE, NIT Hamirpur, Hamirpur, HP, INDIA

Anil Kumar
Dept. of CSE, UTU, Dehradun, Uttarakhand, INDIA

Abstract

Wireless Sensor Networks (WSN) are receiving significant importance in the present scenario owing to their unlimited potential and world wide applications. The routes in the network are determined by the most secured and energy efficient routing protocols and these energy efficient routing protocols employed for WSNs are the Hierarchical or cluster based routing protocols that are essential for path computation in sensor networks. Since most of the hierarchical routing protocols aim to be developed as energy efficient, the security issues are not given much importance most of the times. But in certain applications such as military or battle field the data is to be maintained secret while communicating between sensor nodes and basin so security issues are also required to be focused in developing routing protocols. Keeping in view above in this paper we intend to present the various security issues involved while designing the hierarchical routing protocol for a specific WSN and the design challenges while studying different hierarchical based routing protocols.

Keywords- Wireless Sensor Networks (WSNs), Hierarchical routing, Securityissues.

INTRODUCTION

The hierarchical routing protocols are employed for wireless sensor networks and differ from the traditional routing protocol and are useful in computation of path routing and hence highly affect the performance of the wireless sensor networks. This further indicates that in order to balance the load among the sensor nodes and prolonging the lifetime of a network led to their development. Wireless Sensor networks are emerging as a new tool in various fields such as habitat monitoring in nature preserves, surveillance of buildings as well as in military applications such as for surveillance of enemy activities in battle field and even it is used as tool in gathering events in hazardous environments. At the darker side wireless sensor networks (WSNs) poses a problem in research as a challenge due to their high flexibility in supporting several real world applications which further makes global technical solution difficult to define [2].The core operation of the wireless sensor network is just the collection and processing of the data at network nodes and from these network nodes the necessary data is transmitted to the base station for further analysis and processing. The Routing protocols in wireless sensor networks (WSNs) are mainly classified in two categories:-network structure and protocol operation. Network structure is further classified into Flat, hierarchical and location based routing. On the other hand Protocol operations are further classified into negotiation, multi-path query, QOS and coherent based routing.

- **Routing Basics:** A large number of protocols have been developed to make the wireless sensor networks practically applicable and efficient. These Routing protocols intend to make the constituent sensor network nodes to work in unison to achieve a specific task or multiple tasks in order to minimize energy expenditure and maximize the network lifetime[4].The routing protocol of sensor networks is typically partitioned into two sub routings:-Flat routing protocol and Hierarchical routing protocol. Data aggregation process is performed in the network to avoid the duplicated data transfers. The sequence of such processes forms the basis of hierarchical routing protocol developed as the most energy efficient routing protocols for most of the applications [5]. In certain applications such as military the data is to be maintained secret while communicating between sensor nodes and basin so security issues are also required to be focused along with energy efficiency goal in developing routing protocols. At present there exist several energy efficient communication models and protocols that are designed for specific applications. Moreover the designing of hierarchical routing algorithm includes certain design challenges as well as security issues to be considered for providing secure hierarchical routing in WSNs.

RELATED WORKS

Generally the routing protocols proposed for communication networks are based mainly on network architecture and applications but when it comes to the wireless sensor networks the design objective for research is to obtain the design algorithm that results in the optimal tradeoff between the energy consumption, latency and the data rate for the most of the applications except for few applications like military where security objectives are required to be met as prime objective. While studying the design objective analysis of various hierarchical routing protocols and their applicability to communication networks, we came across the study of design challenges incurred while designing the hierarchical algorithm to achieve maximum tradeoff between the energy efficiency and various security issues involved that further formed the basis of this manuscript or paper In this paper a brief of various hierarchical routing protocols along with the design challenges to be met with to acquire a secured hierarchical routing algorithm for path computation as well as various security considerations to be made while designing the hierarchical routing protocols for sensor networks employing the security applications such as in military surveillances or battle field where the data to be communicated is required to be secure maintaining its integrity as sensor networks routing differs from contemporary communication as well as wireless ad hoc networks.

ROUTING PROTOCOLS

It includes:

3.1 Data Centric Protocols:

Here the queries are sent by the sink to certain regions and these queries wait for the data transmitted by the sensor nodes located in the same region. Since each sensor node transmits data within the deployment region along with sufficient redundancy, the routing protocols must be able to select set of sensor nodes to utilize data aggregation during the relaying of data and overcome inefficient energy consumption.

3.1.1 Flooding and Gossiping:

In case of flooding, each sensor node receives a data packet which is broadcasted to all of its neighbors and this process continues until the packet arrives at the target. Whereas gossiping is an enhancement over flooding in which data packet is transmitted by receiver node to its randomly selected neighbor which further selects its random neighbor to forward the data packet and it continues.

3.1.2 SPIN (Sensor Protocols for Information via Negotiation):

The basic idea behind SPIN is to name the data using high-level descriptors or meta-data. Meta-data uses data advertisement mechanism to exchange data among sensor nodes, which is the main feature of SPIN. Since each node needs to know only its single-hop neighbors, the topological changes are localized which is an advantage of SPIN but this mechanism does not guarantee the data delivery which is the limitation.

3.2 Various Hierarchical Routing Protocols:

The aim of the hierarchical routing is to maintain the energy consumption of sensor nodes efficiently which can be accomplished by allowing multi hop communication within a cluster and then performing data aggregation process. In hierarchical routing architecture the higher energy nodes are used to process and send the information and the lower nodes are used to perform the sensing operation in the vicinity of the target. Hierarchical routing is the two layers routing where one layer is used to select the cluster heads and the other layer is used for routing. [7, 11] .Various hierarchical routing protocols have been developed as fundamental hierarchical routing algorithms employed for wireless sensor network communication. A few of these are:

3.2.1 LEACH (Low Energy Adaptive Clustering Hierarchy):

LEACH is a hierarchical cluster based routing protocol for sensor networks introduced by Heinemann et al [6] It includes distributed cluster formation each with a cluster head and the data arriving from cluster nodes is compressed by the respective cluster heads nodes and then transmitted to base station as aggregated packet there by reducing the amount of information to be transmitted and evenly distribute energy consumption or energy load that is designed with a objective extend the network life time. [2, 3]

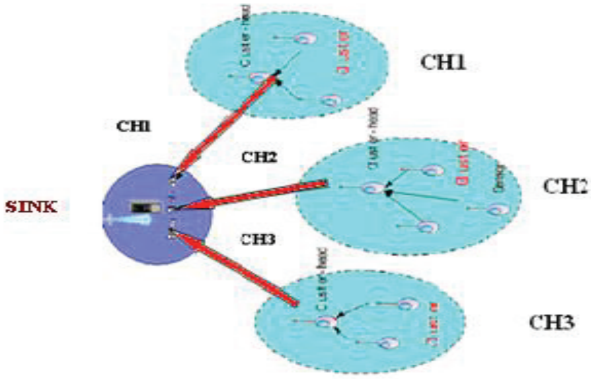


Figure1: Cluster Architecture of Leach

3.2.2 PEGASIS (Power-Efficient Gathering in Sensor Information System):
PEGASIS introduced by Lindsey and Raghavendra [7] is a near optimal chain based protocol developed with two prime objectives:

- Increasing network lifetime which is accomplished by increasing the lifetime of each node in the network using collaborative techniques.
- Reduction in bandwidth consumption while communicating by allowing only local coordination between the closer nodes in the network.[1,2]

PEGASIS improves the performance gain by eliminating the dynamic cluster formation overhead and data aggregation as in LEACH and extends network time twice the amount. In order to reduce the delay it extends to HIERARCHICAL–PEGASIS [5, 7].

3.2.3 TEEN (Threshold sensitive Energy Efficient sensor Network protocol):
TEEN is formulated specially for reactive networks since it responds quickly to the changes in the relevant parameter and transmission occurs only when hard and soft threshold condition are satisfied and developed with aim to reduce the energy consumption. But it has limitation that the nodes will never communicate if the threshold values are not reached and user will not get any data from the network and will not know even if the nodes die. In short it is not suitable for the applications where data on a regular basis is needed [2, 5, 6].

3.2.4 APTEEN (Adaptive Threshold Sensitive Energy Efficient Sensor Network Protocol):
It is developed with a goal to capture periodic data collection as well as reacting to time critical events reducing overhead and complexity problems by implementing threshold based functions. Here Node keeps on sensing the environment continuously and only those nodes that sense data value at or beyond the hard threshold (HT) participate in the transmission providing greater flexibility and control over energy consumption as the design objectives.

3.3 Location Based Protocols:
Location information is needed to calculate the distance between two particular nodes for further estimation of the energy consumption In order to calculate the distance between two particular nodes Location information is needed so that energy consumption can be estimated. These protocols consider the mobility of nodes during its designing primarily for mobile ad hoc networks.

ROUTING ISSUES IN WSN'S

Efficient communication in wireless sensor networks can be achieved if some design challenges are overcome such as: [9].

4.1 Computation Capabilities:
A simple light weight version of traditional routing protocols must be able to meet with WSN communication since the sensor nodes have limited computational power and may fail to run sophisticated network protocols.

4.2 Scalability:
The sensor networks comprises of a set of large number of nodes in the order of hundreds or even thousands so any routing algorithm design must be able to consider such large number of nodes without being affected by the network size, density of nodes and network topology. In other words hierarchical protocols must be sufficiently

scalable to respond to the environmental events in such a way that most of sensors attain sleep state when no event occurs but the moment any event is sensed the system must be able to configure resulting in high quality results.

4.3 Reduced Energy Consumption:

Communication in WSNs is energy conserving as in multi hop communications it acts as data sender as well as data router so the design algorithm must be able to reduce the energy consumption but without compromising the accuracy of the data to be communicated since the malfunctioning of any sensor node even due to power failure can result to topological changes that may need data packets to be rerouted again which further may acquire energy to reorganizes the network.

4.4 Communication Range:

Short transmission ranges are exhibited by the inter sensor communication thereby resulting in multiple wireless hops in a particular route.

4.5 Connectivity:

Sensor nodes are expected to be highly connected since high density of nodes exist in a network and precludes complete isolation from each other to prevent network failure due to node failures for different reasons.

4.6 Adhoc Deployment:

Since sensor nodes are deployed stochastically so it requires that system must be able to cope up with the resultant distribution there by forming connections between the nodes i.e. adaptive system is required which is adaptable to changes in the network connectivity resulted due to node failures .

4.7 Control Overhead:

Control packet overhead increases linearly with node density in a network. This is due to increase in energy consumption and latency caused by the increased number of retransmissions in a wireless medium whenever collision occurs. So the design must aim to obtain tradeoffs among self-configuration, energy consumption and even distribution among nodes and latency keeping the fairness and throughput as secondary importance in WSN.

4.8 Fault Tolerance:

Redundancy at multiple levels may be required in fault tolerant sensor network which further requires active transmission power and signaling rates adjustments on the existing links in order to reduce the power consumption by rerouting the packets through nodes with more energy. This is required since some sensor nodes may fail due to power failure or environmental interferences which in turns affect the network performance. So there must be a provision if any node fails, the routing protocol must be able to form new links and routes to the base station.

4.9 Quality of Service (Qos):

Bounded latency for data delivery is other design requirement for time-constrained applications where data gets useless if undelivered within a certain period of time after the moment it is sensed by the sensor nodes in the network.

4.10 Hardware Constraints:

A sensor node may be smaller than a cubic centimeter and comprises of many hardware components that further consume low power and operates in unattended mode so such to function efficiently and correctly they should be adaptable to the sensor network environment.

SEURITY ISSUES IN WSN'S

In convention security is achieved if every eligible node receives all the messages intended to them, we ensure the security goal if every eligible node receives all the messages intended to it. The significance of security owes to the presence of the resourceful adversary in present scenarios and security goals guarantees the confidentiality, integrity, authenticity, availability and freshness of the data as illustrated below: [11, 12].

- **PRIVACY:** While communicating in the network the data should be understood by the intended recipient only that is the data should not leak by the sensor nodes to the other networks .confidentiality is achieved by the standard technique like cryptography.

- **INTEGRITY:** This means that the data should reach the intended destination without any alteration in the data. The integrity mechanism should ensure that no adversary can manipulate the communicated data since the data loss can occur even due to the communication environment. Message digest and Mac are such techniques to maintain the integrity of the data.

- **LEGITIMACY:** In the network an adversary can be easily introduced so it becomes essential for receiver to ensure the message originated from the correct source and allows receiver to verify that the sent data is authentic that is send from the authorized user. Data authentication is necessary for maintaining the network, coordinating with the sensor node and sending or receiving the data.
- **AVAILIBILITY:** It is required to ensure that the services of the network are available always even in the presence of internal and external attacks such as a denial of a service attack that is DOS. To achieve this goal many mechanisms have been developed.

- **DATA FRESHNESS:** It ensures that the receiver receives the recent and fresh data and also that no adversary can replay the old data and is significant in WSNs where a shared keys are used by nodes for message communications as in such networks a potential adversary can lead to a replay attack using the old key as the new key is being refreshed and propagated to all nodes in the WSN. The mechanisms like nonce and time stamp are added to each packet in order to achieve he freshness of data.

ATTACKS ON ROUTING PROTOCOLS

Most of the wireless sensor networks are developed with energy efficiency as the main goal there by skipping the security issues in mind which can result in various attacks by the consequent adversaries in the network and the main sufferer is the network layer protocol that is the routing protocol. This attack includes: [9, 12].

- **Spoofing or altering or replay the route information:** It includes the routing information corruption launched by an adversary which can attract or redirect the route information there by increasing the traffic as well. This latency further generates routing loops and creates false errors 6.2 Selective forwarding attack: In this mode of attack the malicious node refuses to forward certain packets and drop them simply. If an adversary causes the dropping of the entire received packet, the attack is called a black hole attack and the adversary includes explicitly the path of the data flow to perform the selective forwarding.

- **Sinkhole and wormhole attack:** In both of these attacks the adversaries tries to attract whole traffic from a particular area by means of a compromising node. Sinkhole attack works mainly by making this compromised node look more attractive to the neighbor nodes in order to route the data packets and hence spoofing or dropping the packet there by resulting in various attacks such as selective forwarding, black hole attack or tempering the route information etc. Wormhole attack is caused by an adversary and uses two malicious nodes that try to attract the traffic by showing one hop distance to the sink. Since it uses out-of-bound channel to route packets, the wormhole attack is difficult to detect.

- **Sybil attack:** The Sybil attack is a great threat to many geographic and multipath routing protocols. It employs a single node that presents further multiple identities to the other nodes in the network thereby misleading the node in the neighbor detection, route formation and topology maintenance.

- **Hello flood attack:** The hello flood attack affects the routing protocols that employ local topology like neighbor information for route creation and topology maintenance etc. In this attack an adversary rebroadcasts overhead packet with enough power to be received by every node in the network.[11]

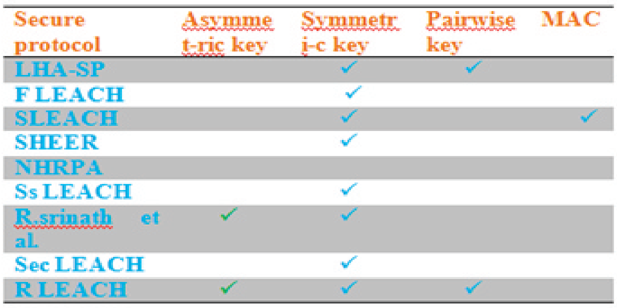
SECURE HIERARCHICAL ROUTING PROTOCOLS

Many previous hierarchical routing protocols assume a safe and secure environment where all sensor nodes cooperate with no attack present. But the real world environment is totally opposite; there are many attacks that affect the performance of routing protocol. Attacker use different kinds of technique to launch attack and damage or harm the data and the network. In order to secure the hierarchical routing protocol many works have been proposed. In this section we discuss those techniques, analyze them and list out the advantages and disadvantages associated with each secure hierarchical routing protocols. [10, 11].

CONCLUSION

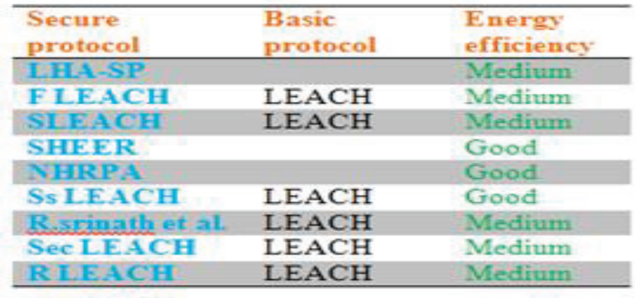
The Wireless sensor networks employs hierarchical routing protocols for the data communication .each algorithm is developed with different design objectives. Most of them are developed keeping energy efficiency as the main goal and few with security issues in mind for applications such as military etc as discussed before. Since the performance of such networks is determined in form of energy efficiency, security, lifetime of the network and resiliency which are further affected by the routing protocols so the efficiency of such sensor networks depends upon the secure robust and efficient routing protocol chosen for the network. In this paper design objectives of different hierarchical routing algorithms is studied and further various security issues and design challenges are discussed which are required to achieve more secure transmission using fundamental hierarchical routing algorithms as analyzed in below table:

Table 1: Security Mechanism Basis Evaluation



Secure protocol	Asymmet-ric key	Symmetri-c key	Pairwise key	MAC
LHA-SP		✓	✓	
F LEACH		✓		
SLEACH		✓		✓
SHEER		✓		
NHRPA				
Ss LEACH		✓		
R.srinath et al.	✓	✓		
Sec LEACH		✓		
R LEACH	✓	✓	✓	

Table 2: Fundamental Aspect Basis Evaluation



Secure protocol	Basic protocol	Energy efficiency
LHA-SP		Medium
F LEACH	LEACH	Medium
SLEACH	LEACH	Medium
SHEER		Good
NHRPA		Good
Ss LEACH	LEACH	Good
R.srinath et al.	LEACH	Medium
Sec LEACH	LEACH	Medium
R LEACH	LEACH	Medium

REFERENCES

"Low Energy Adaptive Clustering Hierarchy with Deterministic Cluster-Head Selection"; M.J. Handy, M. Haas, D.Timmermann; 2002.

"Probabilistic Modeling of Leach Protocol and Computing Sensor Energy Consumption Rate in Sensor Networks"; Song, Dezhen; February 22, 2005.

A survey on routing protocols for wireless sensor networks : Kuan-Ta Lu, Quincy Wu; Date: June 9, 2010.

S. Lindsey and C. Raghavendra, "PEGASIS: Power-Efficient Gathering in Sensor Information Systems".

Manjeshwar and D. Agrawal, "TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks".

Energy -efficient Secure Routing in Wireless Sensor Networks by Shriram Sharma.

Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems by mohammad ilyas and imad mahgoub.

W. Heinzelman, A. Chandrakasan , and H. Balakrishnan. "uAMPS ns Code Extensions".

Routing Protocols in Wireless Sensor Networks Luis Javier Garcia Villalba, Ana Lucila Sandoval Orozco, Alicia Triviño Cabrera and Cláudia Jacy Barenco Abbas.

Hong-bing, Y. Geng, and H. Su-jun. Nhrpa: a novel hierarchical routing protocol algorithm for wireless sensor networks. The Journal of China Universities of Posts and Telecommunications, 15(3):75–81, September 2008.

Shriram Sharma, A.K.Turuk .Energy-efficient secure data aggregation mech- anism for wireless sensor networks, International Conference on International Conference on Emerging and Futuristic System and Technologies (ICE-FST'09),pages 83-87, 09th April to 11th April 2009.

Shriram Sharma, A.K. Turuk .Security in wireless Sensor and Actor classier network., All India Conference on Recent Innovation in Computer Science and Engineering (AICON - 09), 15-22, February 2009.