Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 14 Issue 3 Version 1.0 Year 2014
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

An Efficient Algorithm for Optimization of Power with Computational Security in MANETS

By T. Sukumar, V. Vaishnavi & P. Varsha
Anna University, India

Abstract- The major issues associated with MANETs include the precious battery power of the nodes and security threats from compromised nodes inside the network. The introduction of an additional dynamic node may optimize the power, but however it leads to jamming and interference and thereby reducing the efficiency of the network. Since MANETs have a highly dynamic topology, they are vulnerable to active and passive adversaries. We aim to optimize the network power with added security features and propose a new algorithm "Power with Computational Security (PCS Algorithm)" to overcome the above mentioned drawbacks. The PCS Algorithm employs a dynamically computed "Power Threshold" to achieve efficiency. Also, We make the network secure by introducing a "Security Provider" which consists of dealer phase and combiner phase to ensure all the security requirements are met. Thus, We achieve power efficient and secure data transfer with minimal information and thus it minimizes the mobility, resource and prior-trust relationship constraints.

Keywords: *Ad-hoc, power, MANET, energy and security.*

GJCST-E Classification : *C.2.0*

Strictly as per the compliance and regulations of:

An Efficient Algorithm for Optimization of Power with Computational Security in MANETS

T. Sukumar [α], V. Vaishnavi [σ] & P. Varsha [ρ]

Abstract- The major issues associated with MANETs include the precious battery power of the nodes and security threats from compromised nodes inside the network. The introduction of an additional dynamic node may optimize the power, but however it leads to jamming and interference and thereby reducing the efficiency of the network. Since MANETs have a highly dynamic topology, they are vulnerable to active and passive adversaries.

We aim to optimize the network power with added security features and propose a new algorithm "Power with Computational Security (PCS Algorithm)" to overcome the above mentioned drawbacks. The PCS Algorithm employs a dynamically computed "Power Threshold" to achieve efficiency. Also, We make the network secure by introducing a "Security Provider" which consists of dealer phase and combiner phase to ensure all the security requirements are met. Thus, We achieve power efficient and secure data transfer with minimal information and thus it minimizes the mobility, resource and prior-trust relationship constraints.

Keywords: *Ad-hoc, power, MANET, energy and security.*

I. Introduction

A mobile ad-hoc network (MANET) is a kind of wireless ad-hoc network, and is a self-configuring network of mobile routers (and associated hosts) connected by wireless links – the union of which form an arbitrary topology. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet [1].

The set of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. The design of network protocols for these networks is a complex issue. Regardless of the application, MANETs need efficient distributed algorithms to determine network organization, link scheduling, and routing. However, determining viable routing paths and delivering messages in a decentralized environment where network topology fluctuates is not a well-defined problem. While the shortest path (based on a given cost function) from a source to a destination in a static network is usually the Optimal route, this idea is not easily extended to MANETs. Factors such as variable wireless link Quality, propagation path loss, fading, and multi-user interference, power expended, and topological changes, become relevant issues. The network should be able to adaptively alter the routing paths to alleviate any of these effects. Moreover, in a military environment, preservation of security, latency, reliability, intentional jamming, and recovery from failure are significant concerns. Military networks are designed to maintain a low probability of intercept and/or a low probability of detection. Hence, nodes prefer to radiate as little power as necessary and transmit as infrequently as possible, thus decreasing the probability of detection or interception. A lapse in any of these requirements may degrade the performance and dependability of the network [3] and [4].

a) Routing Protocols for MANETs

A routing protocol is the mechanism by which user traffic is directed and transported through the network from the source node to the destination node [2]. Objectives include maximizing network performance from the application point of view while minimizing the cost of network itself according to its capacity. The application requirements are hop count, delay, throughput, etc; resources residing at each node and number of nodes in the network as well as its density, frequency of end-to-end connection, frequency of topology changes [7] and [8]. The basic routing functionalities for mobile ad hoc networks are:

- *Path generation:* This generates paths according to the assembled and distributed state information of the network and of the application.
- Assembling and distributing network and user traffic state information.
- *Path selection:* This selects appropriate paths based on network application state information.
- *Data Forwarding:* This forwards user traffic along the selected route.
- *Path Maintenance:* Maintaining of the selected route.
- Energy/Bandwidth efficiency.

Author α: Assistant Professor, Department of IT, Sri Venkateswara College of Engineering, Anna University, India.
e-mail: sukumaraser@gmail.com
Author σ, ρ: IT & Anna University, India.
e-mails: vaish_v12@yahoo.co.in, varsha_partha@yahoo.co.in

II. System Architecture

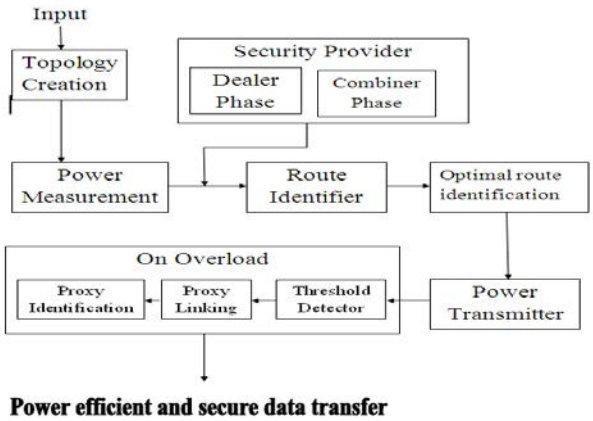

Figure 2.1 : Power Optimizer and Route Identifier Architecture

III. Module Design

a) Topology Design

The first module consists of the basic input details and the processing involved with it to create the network. It requires accurate input data to design the topology of the network. The input details that needs to be specified by the user includes the number of the nodes involved in the design followed by other attributes such as the speed of the data transfer and also the power associated with each node.

On the correct specification of the required details, the topology of the network is generated using the NS2 simulator as shown in Fig.2.2

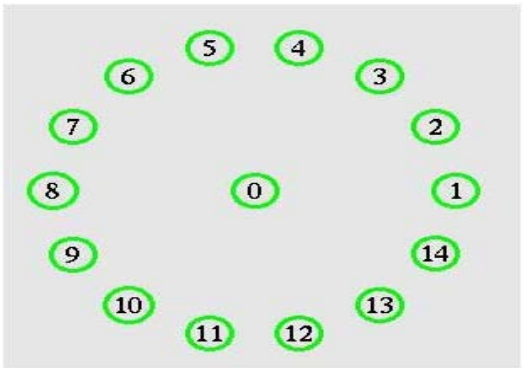

Figure 2.2 : Sample Topology

b) Power Measurement

Every node in the network constantly measures its own power level and keeps track of it and checks for the overload condition. This power measurement helps to keep an overall check of the various nodes available in the network and their respective power levels. Since the nodes in a MANET environment are always in motion, it further helps in recognizing nodes that remain within the range of transmission.

c) Route Identifier

The route identifier is a module that plays an important role in transmission of packets from the source to the destination. For every transmission between a particular source and destination, the route identifier almost immediately generates all the possible paths that can be followed by the source to reach its desired destination. Thus it provides the source with multiple choices to follow. However, in a MANET scenario, since the nodes are mobile, the possibility of predicting the correct route becomes an issue. But the route identifier generates the list on an approximate note and leaves it to optimal route identifier to choose the finally route. Thus, the route identifier merely lists down all the possible routes from a source to its destination.

d) Optimal Route Identifier

The optimal route identifier works as the final authority that decides the final route the source opts to reach the destination. The route identifier aids this cause and list down all the possible routes available and the optimal route identifier analyses the best possible path with respect to the shortest distance and the path that involves the nodes that have enough individual power levels that they can efficiently transmit the information from one end to the other.

e) Packet Transmitter

This module is the fourth module in the PCS Algorithm wherein the nodes route the packets to their destination. This module will execute in the source module. This is of high priority as we are transferring the packets without any loss of information and minimal power consumption being our primary goal.

The source node and its connectivity details along with the path must be known so that the packets can be routed. While transferring the packets it must be made sure that we get acknowledgement for the data sent so that it can be made sure that packet has been delivered to its destination.

The source and the destination node must be alive so that the packets are reached in correct order and safely. Once the packets are delivered in correct sequence, acknowledges must be sent. Also, the power level of the nodes must be checked out so that any node in the path of the packet route does not break down.

f) On Overload

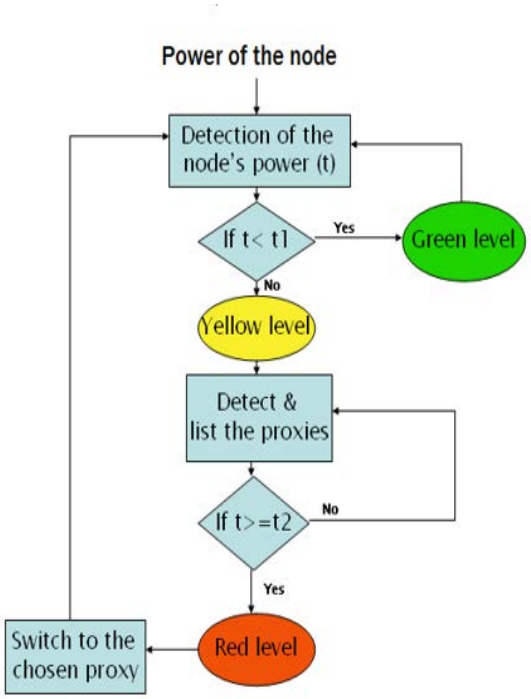

Figure 2.3 : Overload scenarios

This is the most important module of the project as the core job of the PCS algorithm is to route packets through a different path on power failure. The value t in fig 4.4 represents the power level of the individual node. The threshold levels t1 and t2 represents the yellow and red which means that the node is reaching the alarming power levels. This is of the highest priority and depending upon the overload, three cases must be executed. Threshold detection must start when the particular nodes' power level starts drooping. Searching the adjacent nodes must be based on the nodes' power level and also the shortest path and it must display a list of possible paths. Finally, the optimum path must be chosen in such a way that it is both nearer to the source node and also conserves power.

We define three threshold levels: green, yellow and red. As long as the node's power level remains good enough to receive new requests and transmit them, it remains in the green level and continues it process and also keeps a check on its power level simultaneously. Once the initial threshold level is reached, it enters the yellow level, and immediately starts searching for the nodes nearby that can act as a proxy and provide an alternative path. But it can still take receive new requests and process them. But once the power level reaches below the second threshold value, it enters the red level, and requires an immediate replacement with the chosen proxy. Thus, the overload condition is met and is substituted with a proxy node and a new path to continue the processing.

g) Security Provider

The second major issue is addressed by assuming that all nodes in the network have a unique identification associated with them. We assume that there exists a broadcast channel among all nodes in the MANET and if some data is broadcast, each node reads the same value. Hence the attacker cannot try to confuse by sending two different values to different nodes. Every node will be authorized, authenticated, non-repudiated, confident and computationally secure. It involves two phases. A Dealer Phase in which the sender shares a secret among all participating nodes and a Combiner phase where a coalition of size greater than or equal to k constructs the secret. A combination of Chinese remainder theorem, Asmuth Bloom secret sharing scheme and Verifiable secret sharing is used to overcome this problem [6].

The motivation of Threshold cryptography is to share the secret value among multiple individuals called participants (or shareholders) that are engaged in encryption or decryption. The objective is to distribute the secret value in a distributed architecture. This architecture follows the dynamic topology of the networks, in which the participants reside. The secret value is redundantly split into n pieces and is distributed among participants such that t or more than t pieces can recover the original secret value. This is secured message transmission (SMT) between two nodes over n multiple paths in MANET. There are various applications of MANETs, in which TC may be implemented. Applications include coordinating efforts of military attacks in the battlefield or in disaster-struck area, establishing wireless connectivity among various home appliances, and establishing communication among wireless devices such as laptops.

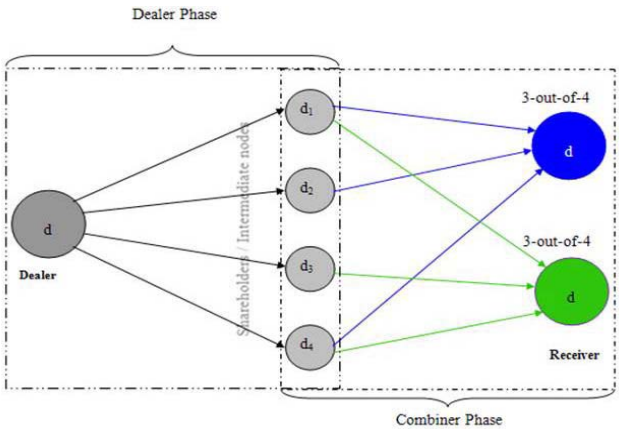

Figure 2.4 : 3 out of-4

Fig.2.4 shows an illustration of secret sharing and coalitions. From the Figure 3-out-of 4, it is clear that for retrieving the message, at least three pieces of shared secret values are required. Hence, the size of coalition is three or more. In this example, the secret value d is split into four parts (n = 4) in the dealer

phase. Then, these split values are broadcast to the participating nodes. After receiving the t (= 3) splitted secret values, the receiver then adds them up and finally retrieves the original secret value.

The benefits of using this kind of secret sharing scheme is that there is no need to know the private and public key components in case of regular RSA[5]. Regular RSA-TC approaches shows that signature generation and verification increases time exponentially when key size is doubled. Also it is computationally secure to generate and distribute consistent shares and it is secure to combine the shares in the reconstruction phase. In VSS, the entire participating node can verify its share in the dealer phase and no node can lie about its share in the combiner phase. Neither the dealer nor the participating nodes can cheat in this scheme. Regular RSA-TC implementation shows that the signature generation and signature verification time increases exponentially when key sizes are doubled. The energy, bandwidth, and storage constraints are important in MANET. So, the RSA-TC implementation is not extremely beneficial for MANETs.

IV. Implementation

a) Algorithm

The PCS algorithm consists of two sections namely the power part and the security provider section. The power section is used to transmit the packets in an energy efficient way. The security provider has two sections namely the dealer and the combiner phase. The algorithm will be defined in detail in the following sections.

b) Power optimizer

To make sure that the packets are transmitted in a power efficient way, we define three levels of threshold value namely the Red, Green and Yellow. The Green level defines that the nodes power is sufficient enough to carry on with the transmission and that no more packets will be lost. The Yellow level means that the nodes power is subsequently falling and that after some point in time it cannot transmit any more packets. It is at this stage where we start searching for proxy node which can carry on the transmission on its behalf. Finally when the Red level is reached, the proxy node is activated, thus reducing the load on the overloaded node and also making a power efficient transmission.

Pseudo code:

START
Nodes n, threshold values t1, t2.
Detection of individual node power t.
If t<t1,
Then green level: continue with the transmission
Else
Yellow level: Detect and list the set of proxy nodes.
Again check if t<t2,
Then continue with the searching of proxy
Else
Red level is reached: switch to the proxy
Continue with the monitoring of power levels.
END

c) Security Provider

All nodes in the MANET have a unique identification. We assume that there exists a broadcast channel among all nodes in the MANET and if some data is broadcast, each node reads the same value. Hence the attacker cannot try to confuse by sending two different values to different nodes. Every node will be authorized, authenticated, non-repudiated, confident and computationally secure. There exists two phases in security provider where the first one being Dealer phase wherein the sender shares a secret among all the participating nodes. Second phase is the Combiner phase where a coalition of size greater than or equal to k constructs the secret.

i. Dealer phase

To share a secret d among a group of n nodes, the dealer does the following:

1. A set of pair wise relatively prime integer's m0 < m1 < m2 <, ...< mn,. where m0 > d is a prime, are chosen such that : $\prod^{t}_{i=1} m_i > m^2_0 \prod^{t-1}_{i=1} m_{n-i+1}$
2. Let M denote $\prod ti=1$ mi. The dealer computes y = d + Am0 where A is a positive integer generated randomly subject to the condition that $0 \le y < M$.
3. The share of the i-th node, $1 \le i \le n$, is $y_i = y \bmod m_i$.

ii. Combiner phase

Let us assume that S is a coalition of t nodes required to reconstruct the secret. Let Ms denote $\prod_{i \in s} m_i$.

1. Let $M_{S\backslash\{i\}}$ denote $\prod_{j \in s\ j \neq i} m_i$ and $M`_{S,i}$ be the multiplicative inverse of $M_{S\backslash\{i\}}$ in $Z^i_m$ i.e. $M_{S\backslash i}\ M`_{S,i} \equiv 1 (\bmod m_i)$.
2. First the i-th node computes: $u_i = y_i\ M`_{S,i}\ M_{S\backslash\{i\}} \bmod M_S$
3. The nodes then compute $y = (\Sigma_{i \in S} u_i) \bmod M_s$ for $i \in S$, solve y in Z_M using CRT.
4. It is required to compute the secret d using d = y mod m_0. According to CRT, y can be determined uniquely in Z_M since $y < M < M_S$ the solution is also unique in Z_M.

If all shares are valid, the participating node can obtains secret d by using the reconstruction procedure of Asmuth- Bloom Secret Sharing Scheme otherwise, malicious nodes are disqualified.

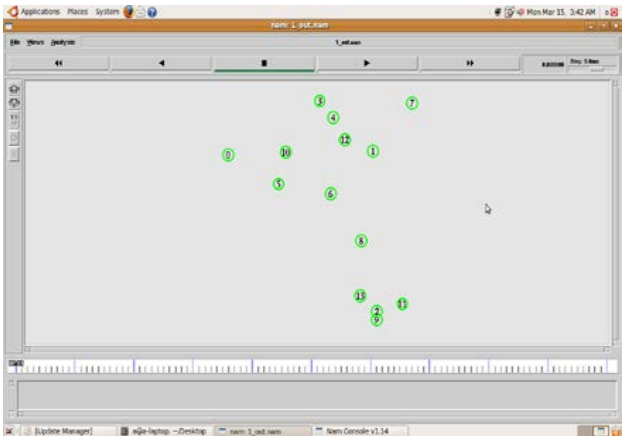

Figure 3.1: Topology Creation

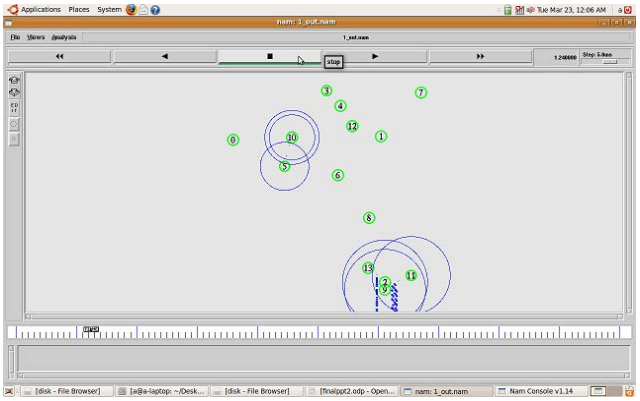

Figure 3.2 : Node 10-5 and 13-11

This figure explains two things: the power overload condition and the work of malicious node. Here the circles represent the transmission range and the small falling thing represents the loss of packets. Here node 10 is transmitting to node 5 which represents normal transmission. Also node 13 wants transmits to 11. But according to the security provider algorithm, it is detected that node 2 is malicious and hence it does not transmit the packets. Since node 2 is found out to be malicious, node 13 starts looking out for alternate way of transmitting to 11 which will both be power efficient and secure way.

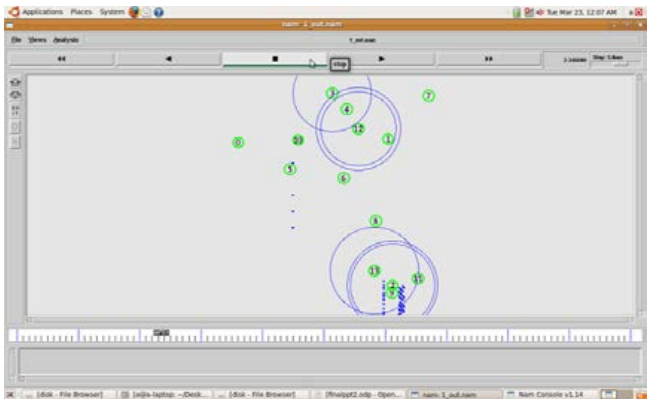

Figure 3.3 : Node 5 is overloaded

The node 13 is searching for the alternate way of transmitting the packets. But the main thing to be noted here is node 5 is overloaded, i.e. it can no more transmit any packets. Node 5 has attained the yellow threshold level. Node 5 now searches proxy node to receive all its packets. If this is not done then the packet starts losing its way. Also, now node 12 wants to transmit to node3. According to the PCS algorithm it searches for the path which is secured and discovers the path as 12-4-3 which is in accordance with the PCS algorithm.

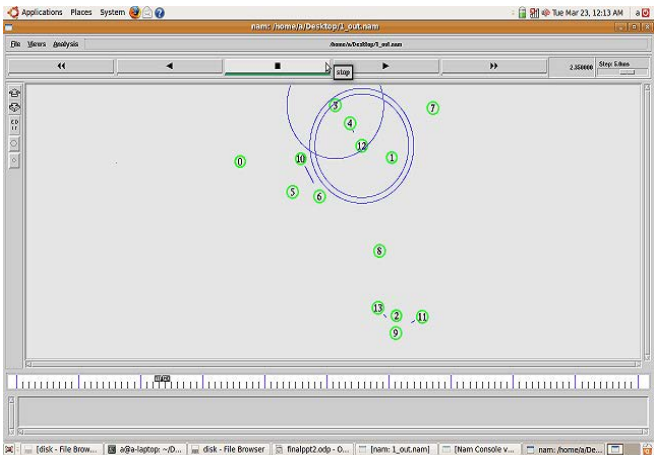

Figure 3.4 : Nodes 10-6 and 13-9-11

Since node 5 is overloaded, it finds out suitable proxy which is nearby and has the power to carry out transmission. Thus it locates 6 as the proxy node. Thereafter node 10 transmits the packets to node 6. Since node 2 is malicious and node 13 sends the packet to 9 which then forwards the packet to node 11. Thus the malicious node is removed and also the overloaded node is taken off from its overloaded conditions. Node 10 will transmit to node 6 until node 5 is charged and gets back its power.

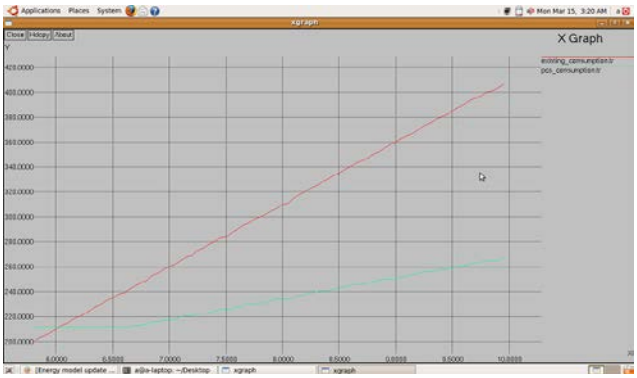

Figure 3.5 : Comparison of Existing and PCS algorithm

The performance of PCS algorithm is studied by plotting the x-graph. The nodes are put under different load conditions at different point of time. The outputs are analyzed using the trace files. The power levels are

plotted against the number of nodes to which packets are forwarded and the x-graph is plotted. The graph shows that pcs algorithm is way efficient than the existing method. Initially for less number of nodes the existing algorithm may seem efficient but as the number of nodes increases the performance levels drops down. In a network generally the nodes will always be overloaded. Hence the new methodology seems to fit in the place perfectly.

V. Conclusions

The performance of PCS algorithm is studied under NS2.30. Effective simulations are carried out many times for different traffic and the trace files are studied. TCL scripts are written to find out the throughput. A comparative study of the proposed and the existing technique has been depicted using an X-Graph which is plotted to show the power consumption on overload conditions. The graphical results show that it results in a power efficient and secure data transfer. The proposed algorithm has the following benefits associated with it:

- With the introduction of the concept of threshold and proxy, the interference is considerably reduced and hence the capacity of the network is increased.
- It comes across as a suitable replacement to the traditional routing schemes as it aims at a energy cum security approach to meet the existing problem,
- In addition, there is no need to know the private and public key components in case of regular RSA and thus it becomes more difficult to crack.
- It is also computationally secure to generate and distribute consistent shares.
- Additionally it's secured by combining the shares in the reconstruction phase.

a) *Future Work*

The PCS algorithm is almost two times more efficient than the existing technique. But however it can be further enhanced to improve upon the efficiency level and be applied to a broader spectrum. The following are the suggestive methodologies that can be improved further:

- The performance of the nodes with respect to the power efficiency can be improved with the introduction of multiple proxy nodes.
- This concept of simulation can be further extended to a multicast routing environment.
- The security can be further ensured by embedding ID based cryptography in the present scheme and thereby making the network a safe haven.
- Efficient modeling of the power consumption characteristics of wireless networks using simulation tools requires accurate WLAN model. Here we have shown that the insight obtained from NS2 simulation is of greater value while designing and analyzing the energy models.

VI. Acknowledgment

We would like to acknowledge Michael Shell and other contributors for developing and maintaining the IEEE LaTeX style files which have been used in the preparation of this template.

References Références Referencias

1. Ertaul.L and Chavan.N. "Security of Ad Hoc Networks and Threshold Cryptography" International Conference on Wireless Networks, Communications and Mobile Computing,2006.
2. Fabian Kuhn, Roger Wattenhofer, Aaron Zollinger. "An Algorithmic Approach to Geographic Routing in Ad Hoc and Sensor Networks". IEEE/ACM Transcations on Networking VOL. 16, NO. 1, February 2008.
3. Fan Wu, Tingting Chen, Sheng Zhong, Li Erran Li, and Yang Richard Yang. "Incentive-Compatible Opportunistic Routing for Wireless Networks" in MOBICOM 2008, Proceedings of the Fourteenth Annual International Conference Mobile Computing and Networking Pages 303-314.
4. Ishai Menache and Nahum Shimkin. "Capacity Management and Equilibrium for Proportional QoS". IEEE/ACM Transcations on Networking, VOL. 16, NO. 5, October 2008.
5. Jiqiang Liu and Sheng Zhong. "Analysis Of Kim -Jeon-Yoo Password Authentication Schemes" Cryptologia, Volume 33,Number 2, Pages 183-187, 2009.
6. Kaya C.K and Selcuk.A.A."A Verifiable Secret Sharing Scheme based on Chinese Remainder Theorem". INDOCRYPT 2008.
7. Manel Boujelben1, Habib Youssef2, Mohamed Abid. "An efficient scheme for key pre-distribution in wireless sensor Networks". IEEE International Conference on Wireless & Mobile Computing, Networking & Communication, 2009.
8. Weifa Liang, Richard Brent, Yinlong Xu, Qingshan Wang. "Minimum-Energy All-to-All Multicasting in Wireless Ad Hoc Networks". IEEE Transcations on Wireless Communications Vol 8, No:11, November 2009.
9. http://www.isi.edu/nsnam/ns/tutorial/
10. http://en.wikipedia.org/wiki/Network_simulation
11. http://nile.wpi.edu/NS/
12. http://en.wikipedia.org/wiki/C (programming_language)
13. http://www.tclscript.com/index.shtml

Global Journals Inc. (US) Guidelines Handbook 2014

www.GlobalJournals.org