Robust security in wireless network with Loop Trace monitoring Approach

Md. Zainlabuddin, R. P. Singh

Abstract: Security concern in wireless network is a prime issue to overcome to offer better service quality for next generation applications. To offer robust security in wireless network, a optimal loop trace monitoring approach for security provisioning in wireless network is proposed. the approach offer a monitoring of the secure data exchange and builds a security measure to declare the reliability of the node. The communication packets are then chosen based on the offered security value and the route selected. A higher offering security level route is chosen in data exchange for reliable coding. The simulation results were carried out for the existing reliability factor of data exchange over the proposed approach of loop trace monitoring to validate the proposed work.

Index Terms: Secure coding, wireless network, loop trace monitoring and robust reliable coding

I. INTRODUCTION

Security measure is needed to guarantee the offered service quality in evolving wireless network. In the development of security protocol in wireless network, key scheduling and authentication are more dominantly observed. To develop security objective various past works were seen. In [2] a new position based routing protocol is developed by the Unknown anonymous Routing Protocol (AO2P). In this AO2P, the location of the target is encrypted using a common key of nodes, and is used as routing encrypted information. [3] Specifies a security protocol called PRISM. This approach develops tracking-resistant mechanics for managing secure data exchange. Such methods offer a privacy approach because they depend on some environmental factors, such as network size and a variation of mobility patterns. These tasks are defined as the nodal tracking in defensive and node resistance is offered by achieving centralized management routing in a private friendly network. Location cloaking specifies geographical ad hoc routing protocols to eliminate such a problem is outline in [4], introducing a new concept called secure link. A network link refers to a secure link if the packet delivery for a sender and the location resolution of the receiver. However, in such coding approach, the location radius causes a concern of packet forwarding. Packets can be forwarded only if nodes are in contact, which can result in reduction in network output and overhead increments.

To avoid such limitations, [5] presented a safe, efficient and an interactive access protocol for temporary MANETs. It was built using the Bivariate polynomials based secret sharing techniques. MANET introduces a method to set up secure communication channels in nodes. This approach has a public key function which does not have any node certificates. The inspection policy uses secret confidentiality as a major distribution plan and shares the secret as private keys. In [6] a major management is introduced for the safe route. This routing ensures successful routing between unauthorized nodes with negative nodes around the network, and ensures a base of the secure MANET system. Location-based service management protocol (MRLSMP) was introduced in [7] where a location service management protocol aims at tracing the result of deploying organized frameworks, in order to control location information, using geographic clustering is proposed which enhances the messaging aggregation. A Hybrid network is presented in [8] as a lightweight protocol to protect the route, data transmission, and user privacy at the adhoc wireless network. In this approach to keep users anonymous, the publishers use the session key. However, the Key is of allotted time, so the relativity of the attacks increases. In [9] a lightweight privacy protocol that ask for source name and routing privacy is presented. This method presented a reactive routing and exchange message only when a need to send a message is made. This approach reduces the network overhead, however the dynamic key selection leads to a question on its suitability. As the keys are dynamically selected the validation of the key for non-repeating or security factor is not investigated. However, to get a security component, it suggests a script cryptography for building decentralized access control mechanisms for AdHoc network. This instruction includes adhoc network access control mechanisms and group security policies. However, this activity is only associated with access control and does not address the specification and discussion of the Group Safety Policy. Though various keying mechanism or authentication schemes were developed they suffer from a problem of distributed architecture and imbalance usage of storage resources. The load balancing issue addressed in [11] provides an innovative way of addressing the problem. Calculations with a specific hash function is made instead of changing the geo-routing protocol to indicate the target position of a search result. This approach is a particular approach to the security system distributed. Using information on nodes from positional systems such as GPS, in [12] a dynamic condition in the routing protocol is proposed.

Manuscript published on 30 March 2019.
***Correspondence Author(s)**

Md. Zainlabuddin, [1]Research Scholar, Sri Satya Sai University of Technology and Medical Science, Bhopal, Madhya Pradesh
Dr. R. P. Singh, Research Guide, Sri Satya Sai University of Technology and Medical Science, Bhopal, Madhya Pradesh

In such code, location information will be shared based on the node identity broadcast.

Broadly casting overhead is ignored in such an approach. Towards trustiness coding in distributed networks a framework is outlined in [13]. By investigating correlations and differences of establishing trust in social context the trust in distributed network is made and trust metrics are developed. The process of trustiness presented is based on the content of the data; however the security concern due to geographical location is not evaluated in such approach. To achieve the objective of providing a infrastructure free secure routing protocol A Safety management help introduce inter-nodular periodic broadcasts for observation of node behavior. An advanced method called a geographic hash has been suggested in [14] for encoding which provides unforgiving geographical information. It is a broadcasting approach that focuses attention on the safety of the place. In [15] to achieve a similar goal on an unknown routing protocol, a protocol called ARAKE is proposed where the sender and receiver is not only anonymous, but also defined intermediate nodes from the network at the same time. [16] suggested a fixed invasion to identify the number in the node. In this approach an anonymous MAC and network layer communications are defined, which is called as MASK. This approach uses dynamic pseudo codes rather than static MAC and network ID. The source location is a derivation routine scheme introduced by a tree [17] while treating the source location and maintaining a lifetime within the wireless networks referred to as the tree. This approach is as well, a routing security method which maximizes the network life time by evaluating the redundant information and in accordance code for tree routing to achieve longer operational life. In [18] an efficient and extractive tools for an advanced routing for authentic routines is outlined. in [19] focus on routing using a single radio interface for Data and Control SMS Exchange is presented. The main problem noted is the control system which is used to broadcast to all nodes in the network taking time, which increases time consumption and increases network overhead. To achieve a similar objective of high data transmission, a load balancing approach is proposed in [20] to avoid the load balancing in ad-hoc network congestion on the demand distance vector (LB-AODV) protocol. A rounding metric has been designed to indicate the path load condition. In [21] In addition to power allocation a route selection approach is performed at the destination. It is a hybrid approach of routing where PUs and SUs are together used for route establishment. This introduces initial delay at route establishment. In [22] the channel assignment and route establishment in cognitive radio networks through a combination of rounding and channel assignment is proposed. however this approach increases the overhead in the network. A new far-off regional Geo casting Scheme is proposed in [23] for multi-hop wireless network and does not require nodes to interpret the geographical location of them. In this approach a blind flooding over a required geographical region is presented. This is focused to reduce the broadcasting effort. While in [24] for location privacy a data sink privacy at the sink with backbone flooding is proposed. the conventional approaches however were not able to derive a secure modeling of data exchange over the network in a authentic reliable manner. To present the developed work, this paper is outlined in 6 sections. Section 2 defined the conventional approach of reliability secure coding in Adhoc network. The proposed solution of Loop Trace monitoring Approach is outlined in section 3. Section 4 outlines the experimental results obtained, the concluding remarks are made at section 5. Section 6 outlines the references used.

II. SECURE RELIABLE ROUTING

The issue of revoking the certificate on the AdHoc network has been challenging since the trusted authorities in such network do not have access by a on-line access. In Wired Network environments, Certificate Authorities (CAs) generates a certificate revocation lists (CRLs), collect information, and post on repositories accessible or distribute to relevant nodes when certificates are canceled. In general, ad hoc networks, usually do not have access to centralized repositories or trusted authorities; Therefore, cancellation or acceptance of certificates does not execute. Another challenge is the adjustable network security that is either self-reliance or security routing in the presence of an attack by an intermediate node. These nodes or conflicting activities interfere with network traffic and cause various communication issues. Figure 1 illustrates a simple example of how nodes in wireless adHoc network performs a security task.

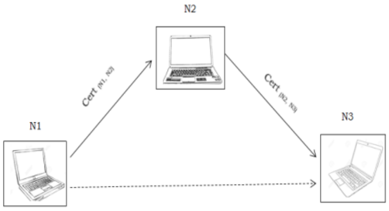

Fig.1: Security data exchange in adHoc network

In figure 1, N_1, N_2, N_3 issues certificates, as a packet is specified as public key pkN_i. A certificate has been issued to N_2, indicating that PkN_2 include the N_2's public key. N_1 taking N_2 as reliable will buffer all the certificates as trusted. However, these certificates are to be validated with the forwarding of packets to declare it as reliable. To Perform a reliability test, N1 exchange the security certificate of N2 from N3. The two security certificate, from N2 and N3 are matched to declare the authenticity of the node. If the correlation is observed to be negative, the security certificates will be validated. With creation of new certificates, Certificate Exchange continue even in the data exchange mode. Node's non-modified repositories are constantly updated with new certificates. After this, the node creates a repository of its modified certificates. Node, communicates with its certificate graph. If the node reports its modified certificates, it is ready to ensure authenticity. For security reasons, it is usually the basis for authenticity, integrity, confidentiality, denial and availability, authentication of communicating nodes, and other security objectives.

For example, in a communication, those nodes who have not previously verified their identity, authentication can be done in multiple ways using a symmetric or asymmetric cryptographic algorithm. In symmetric algorithms preshared key exists (not present in public conditions), authentication via asymmetric cryptography requires public safety mapping Public Key Infrastructure (PKI) Keys to identifiable owners identities.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

PKIs use digital signature certificates to verify the identity of a key owner. A user must prove their identity as a Certification Authority (CA) and a digital signature certificate that will prove to be owned by her public key. But the main problem regarding any service designs on adHoc networks is not have dependent on any of the institutions that are centralized because such institutions are easy to attack, and all the network's partners cannot always ensure their accessibility.

Therefore, a public keying mechanism cannot implement a centralized and trusted institution as introduced in the local area networks or on the Internet.Instead, a distributed solution over a wide distributed adHoc network is to be developed.

Each node can reach a particular node or mobile users in a adHoc network. Every mobile user interact with other users in its communications ranges. Every mobile user has its own power, to create packets or messages via wireless link to reach other users. Depending on the energy, there is a certain limit or distance where each node can communicate. This is termed as communication range, defined as a distance of nodes in the communication range. Here, any node can send messages to the nodes inside its communications range. Nodes in the communication ranges can be found by packet broadcasting. Nodes that falls within the communication range are directly connected and termed as neighbor nodes. Wherein data are exchanged for a neighbor to neighbor nodes. In a security coding called ‘threshold cryptography’ the nodes are detected from all other nodes based on node coverage probabilities and the node with highest coverage is declared as the head or server of the group. All other nodes are the registered node to this node considering as a server node. In the security provisioning each user generates its own public key, which is used for encrypting messages or to communicate. The main issue of any public key security is that access to the public key for each user is made available to others by its authenticity. The centralized server node is believed to be a reliable node. All nodes send their public keys to the server node. The server node or cluster head accepts the public keys of all nodes. This forms a repository table with these keys. This repository table contains details about each node, namely ID for public key for each node. The node can know the public key of any other node in the network by communicating with the server's node. Each node is believed to be on this centralized server node and believes that any information provided by this node is reliable. Nodes on the network change their public key, and update is sent to the server as a new public key. This enables a centralized server node to retrieve updated information about the nodes key on the network. Threshold based cryptography method is a centralized node for observing keys. Exclusive distribution and authentication depend entirely on a centralized node. Any failure in the key generation results in incorrect authentication. All nodes are in a centralized node to ensure authenticity. When interacting two nodes, each intermediate node and a public key of the next node is selected optimally based on the route connect and the key is referred from a centralized node. Delaying delivery of this key request result in communication delayed. This affects the exchange rate of packs. In addition, it is very difficult to establish a key management service using a server node on adHoc networks. The server node, responsible for network security, is a vulnerable point of network, if the node is unavailable, the remainder of the nodes cannot secure the current public keys of other nodes or offer a secure communication with others. If the server's node is disconnected from the private key of the node, the attacker can easily enter to the network.

III. LOOP TRACE MONITORING APPROACH

In the proposed approach, third party and public keys are not authenticated as traditional public key infrastructure solutions. Instead, each user has the ability to test other users' public keys. Each user will be link up to each other user to decide how much a node trust on a particular certificate. The system's initial phase is implemented in three phases: each node creates a public / private key pair, distribute certifies to every node, provides certificates to other nodes and produce an updated certificate repository, Certificates exchanging nodes, and Create an updated repositories. Each of these steps are depicted as,

Step-1: Generation of public/private key sets

Each node defined a set of private and public key.

Step-2: Key Distribution

Each user depends on the power level defines the user's communications range. Depending on the communication range of nodes, it detects the neighboring node in a single-hop range. Once the nodes create their public keys, the key are delivered. During the broadcast period, each user uses its closest neighbors. This is a synchronous process, which means it happens simultaneously on each node. All users now on the network were made aware of the general public keys of their neighbors.

Step-3: Certificate issuing

Each node gets its neighbor's public keys. A neighbor node obtain a public key, as a certificate containing a node ID and a public key. This Indicates that the node believe in the identity of the sender. Each node is recognized as a sending node with the certificate of the received node key. All nodes on the network are processed at the same time.

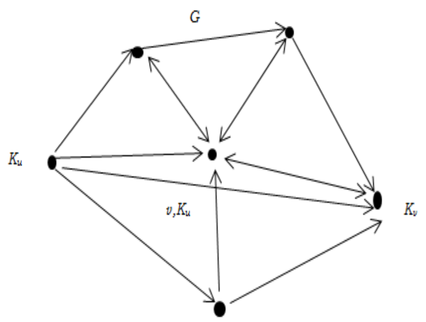

Fig.2: Key exchange process

Certificate issued is of the following form. It consists of id’s and public keys of the two nodes involved in exchange of certificates.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

Each node collects certificates from a neighbor. Exchange certificates are saved in the form of a repository table in each node. In the node issue a certificate this certificate node and its public key provide node ID and public key PIN. The authentication of the given key is provided by the key received. By checking the second field of the certificate issued by the node M, the key determine the authenticity of the node. That is, by its own key. The node believes that node has a valid public key and can communicate. Certificate Exchanges in a hop fashion locally, the Certification Exchange process has a minimal communication cost and each node stores the repository list in its memory. The following is the form of the non-modified repository table,

Table 1: certificate repository table of a node

N id	N key	S id	S.key
m	Pm	K	Pk
m	Pm	L	Pl
m	Pm	N	Pn
m	Pm	O	Po

Step-4: Repositories updation

Every network has the operational period to run a network for network setup. This work cycle is known as a beacon period. The period of this beacon includes time to start and communicate with the network. Start time is about the time taken for nodes to know about all other nodes in the network. This period is called a broadcast period or setup period. During this period, the nodes exchange their public keys, collected certificates of one-hop neighbor and created repository tables. When communicating with two nodes, an optimal route using a selected routing algorithm is done. The source that want to communicate, passes a public key to the next node on the route and starts communicating with its key from the repository table. Using the public key for the next node a encrypted message to encrypt the source of the message is made. figure 3 illustrates the key exchange mechanism.

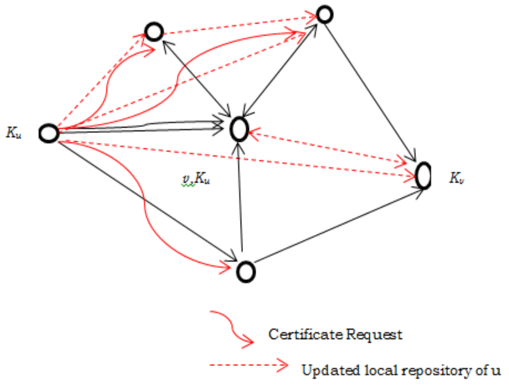

Fig.3: key exchange process

Because mobile adHoc networks are random, all nodes may be discarded on a network or new nodes may join the network at any instance. Nodes or users will continue to change their location in such network. So, the network is dynamic in nature. Changes occurring on network during the beacon are not considered until the beacon completes. This does not affect the current communication and remain intact with the changes applied. Once the beacon expires, the repository list taken as a backup for each node. Then for every beacon period each node find their neighbors. These neighbors may be the same as those encountered by a node in the previous network, or may be a new updates added to the network. For the new network, Public keys and certificates are refreshed. Getting a new certificate on the initiation the node, checks whether a backup repository table has the same certificate or any new updates exist. If it already has the same certificate in its backup the repository list will remain unchanged, however, the newly-accepted certificate for the added nodes will be verified and added to the network. All final certificates are maintained in the new repository table for certificates issued by the nodes present in the network. With ease of public key binding, other users can cancel their issuing certificates. Likewise, users can override their own certificates if they believe their private key is compromised. This new repository table is refreshed as a updated repository table. This reduces the amount of time for the updation of the repository table. This repository are used as the new certificate unit for data exchange. This has a advantage of lower repository overhead and retaining the security measure for dynamic node variation.

IV. SIMULATION RESULTS

The developed approaches are validated for the performance measure. Three analyzing factors are used namely,

- Propagation delay
- Average packet delivery
- Repository updating factor

a) Propagation delay:

The propagation delay is defined as the time to transmit a packet in communication from a source to sink.

This factor is compared for the two developed methods. Comparatively the self organizing cryptographic approach gives lower propagation delay than the threshold cryptography approach in data propagation with security key coding. the signaling delay for a threshold cryptography is higher for key exchange.

b) Average packet delivery:

Average packet delivery is the number of packets delivered to a node in the network. This depends on the time taken from the source node to generate, propagate and buffer packet at the destination node. Testing for various packet sizes, the packet delivery for packet transfer in both cases is computed. **This factor** looks more improved for self-organization approaches when compared to the threshold cryptographic approach. the average packet delivery for the network is defined by,

$$Average\ packet\ delivery = \frac{packet\ generated\ for\ source}{packet\ recived\ at\ a\ node}\ over\ ti \qquad (1)$$

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

c) Repository updating factor:

This factor defines the updates as the repository component as the size of the repository table after each beacon period. Reducing the amount of the repository for each beacon period. The updation indicates that there is no need for large memory to store repository tables in a node. This gives ad hoc network an additional benefit if the limited amount of memory resource is available.

Table 2 illustrates the network parameter used in simulation for the developed approaches.

Table.2: Network parameters for simulation

Parameter	Values
Nodes in network (n)	20
Network Simulation area	200 x 200
Offered bandwidth to node	Random
Routing	DSR
Route optimizing	SWP
Network layout	Random

In the analysis of the developed security algorithm, the proposed approach is compared with the security coding approach of secure routing protocol (SRP) [26], threshold cryptography (th) using central key distribution [25], and the proposed self optimizing repository (SO) updation. To validate the developed approach, different network layouts are simulated with variation in the offering load and node density in the network. The suggested approach are validated for the above three measuring factors as stated above. The result obtained are presented as below,

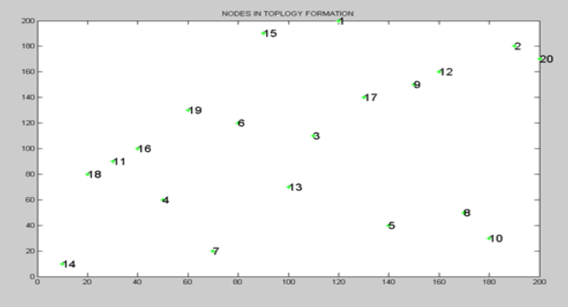

Fig.4: Network layout for simulation

The network is simulated for the network values variation of nodes, offered load and the variation in source and destination. The observations obtained are,

Test-1

Packets exchanged : 1 Kbyte
Source ID: 18
Sink ID: 12
Selected Route : 18, 4, 6, 17, 12

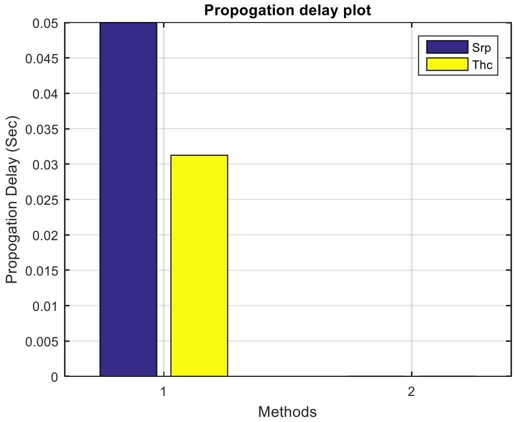

Fig.5: Propagation delay plot

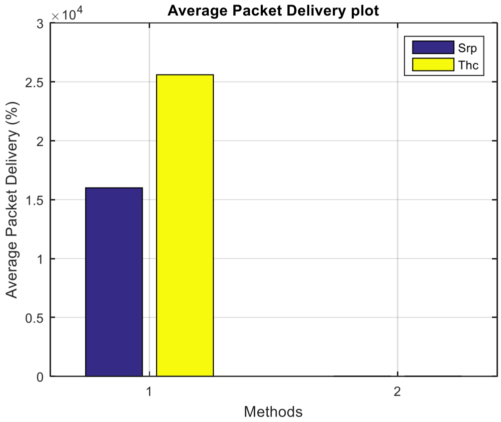

Fig.6: Average packet delivery

The average delay and propagation delay observed are illustrated in figure 5, 6 respectively. This delay is minimized by a factor of 0.02 Sec, and the packet delivery is improved by, 1.1 Kbyte. To evaluate the effect of measuring parameter over path variation, the source and sink nodes are varied over the same network and the parameters are observed.

Test- 2

Packets exchanged: 1 Kbyte
Source ID: 14
Sink ID: 20
Selected Route: 14, 4, 6, 3, 9, 20

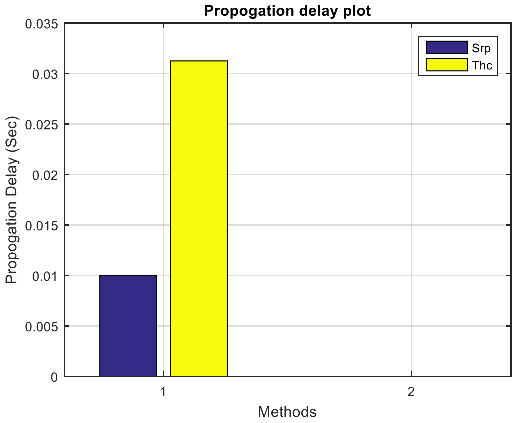

Fig.7: Propagation Delay

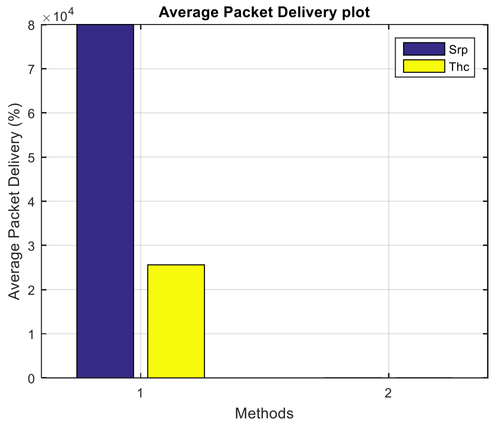

Fig.8: Average packet delivery

The delay is lower by 0.02 sec and the average packet delivery is improved by 5.8 Kbytes. On the same path the offered load is varied to observe the impact of offered load on the network. the test case parameters is as outlined,

Test-3

Packets exchanged: 4 Kbyte
Source ID: 14
Sink ID: 20
Selected Route: 14, 4, 6, 3, 9, 20

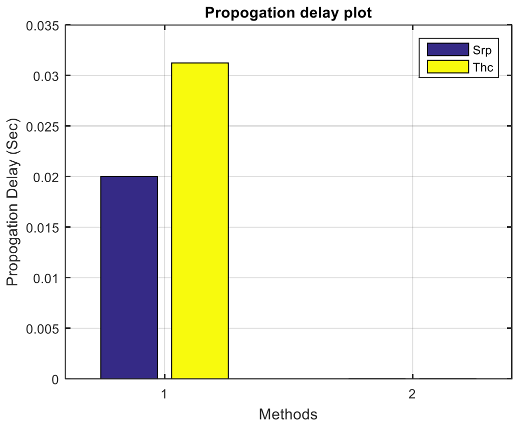

Fig.9: Propagation delay

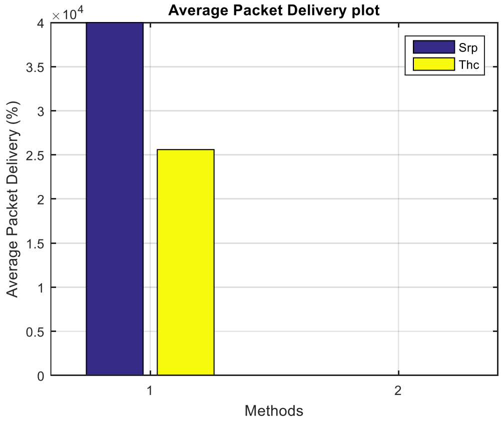

Fig.10: Average packet delivery

Test 4

No. of add on Nodes: 2
Packets exchanged: 4 Kbyte
Source ID: 14
Sink ID: 20
Selected Route: 14, 4, 6, 3, 9, 20

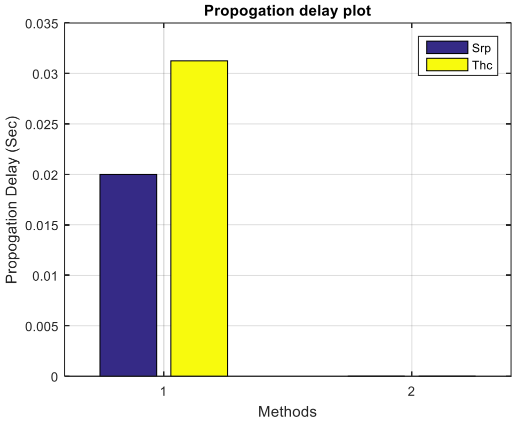

Fig.11: propagation delay

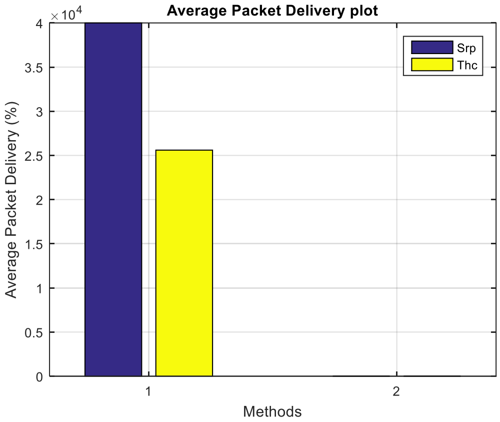

Fig.12: Average packet delivery

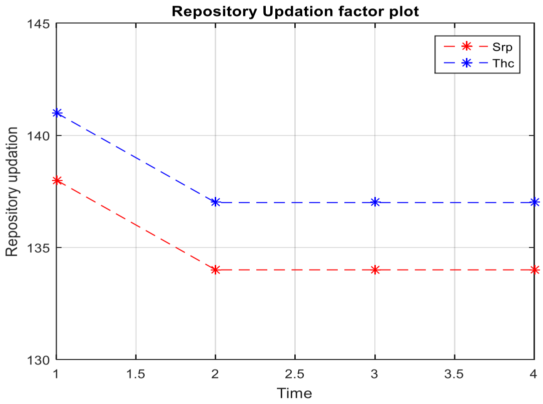

Fig.13: Repository updating plot

Test 5

Node variation: 2 added, 1 removed
Packets exchanged: 4 Kbyte
Source ID: 14
Sink ID: 20
Selected Route: 14, 4, 6, 3, 9, 20

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

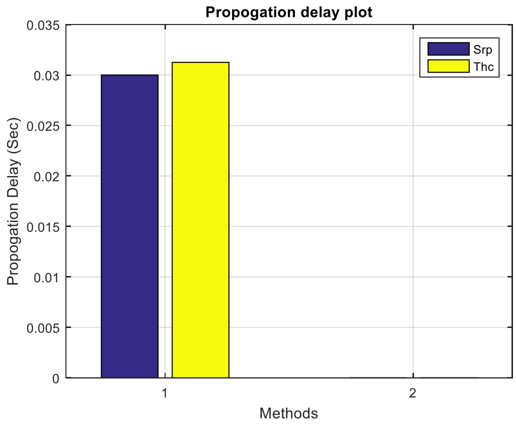

Fig.14: propagation delay

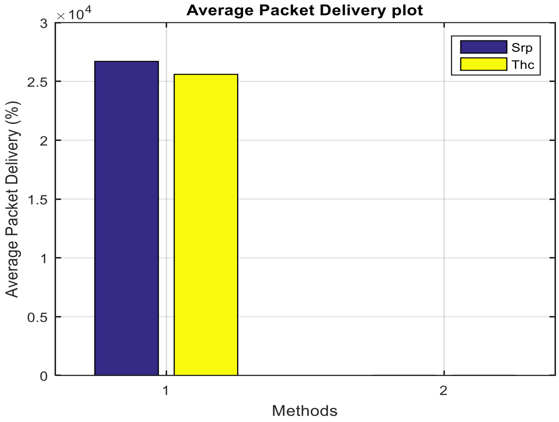

Fig.15: Average packet delivery

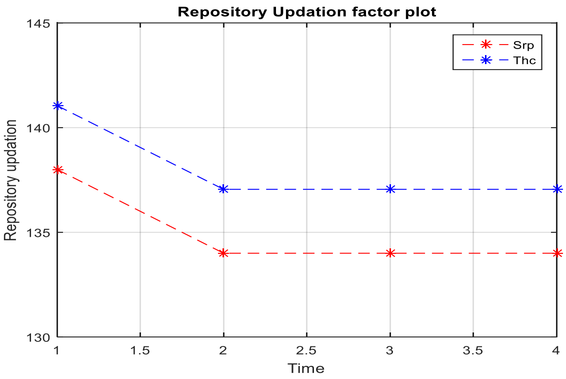

Fig.16: Repository updating plot

Observation show the robustness of proposed approach, it was tested over various network environments and evaluated the performance via some performance metrics. The performance metrics considered for evaluation are signaling overhead, traffic blockage, throughput, power consumption and the network life time with varying node density and with varying packet size. The obtained performance metrics for the proposed approach is shown below. Comparative analyses are also carried out between the proposed self-organized cryptography (SOC) and the conventional threshold cryptography (THC) and secure routing protocol (SRP).

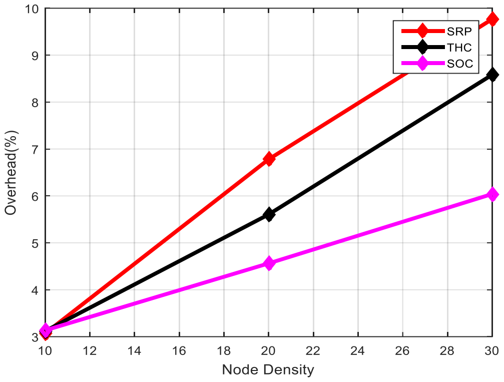

Fig.17: Signaling overhead for varying node density

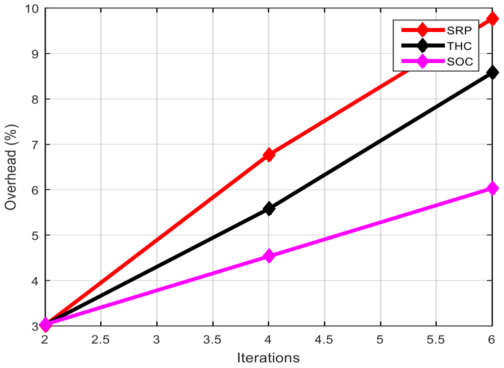

Fig.18: Signaling overhead for varying packet size

In case of signaling overhead, the proposed approach must have less signaling overhead.

This can achieve by reducing the number of control packets transmitting between the nodes during communication. The signaling overhead will be increased when there is an increment in the node density and also the packet size. The observation illustrates that the proposed approach has less signaling overhead compared to THC and SRP. Since the proposed approach provides security with less number of control packets, the signaling overhead is less.

Table.3: Routing overhead evaluation with respect to control packets with varying node density

No.of nodes	SRP	THC	SOC
10	333	325	310
20	710	605	458
30	1020	930	634
40	1150	1020	711
50	1206	1050	732
60	1258	1080	758

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

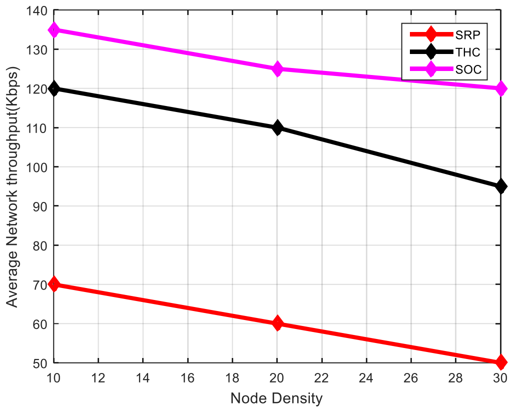

Fig.19: Throughput for varying node density

Figures 19 and 20 illustrate the performance of proposed approach through the achieved throughput for varying node density and varying packet size. with the node density increment, the throughput will be decreased due to the blockage at particular node. Since the proposed approach resist the attacks more efficiently, the throughput of the proposed approach is better compared to conventional approaches.

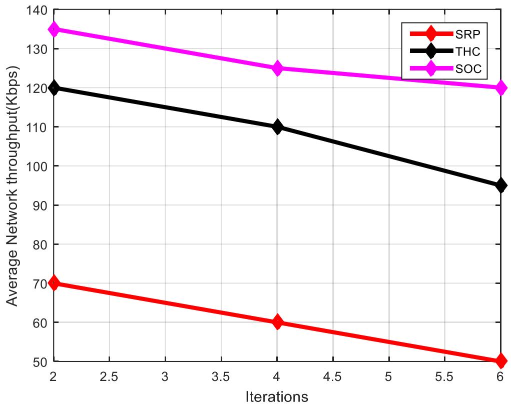

Fig.20: Throughput for varying packet size

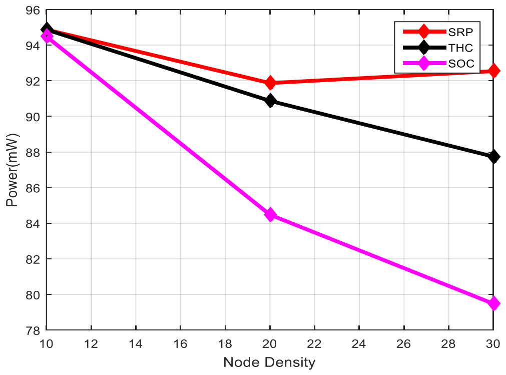

Fig.21: Power for varying node density

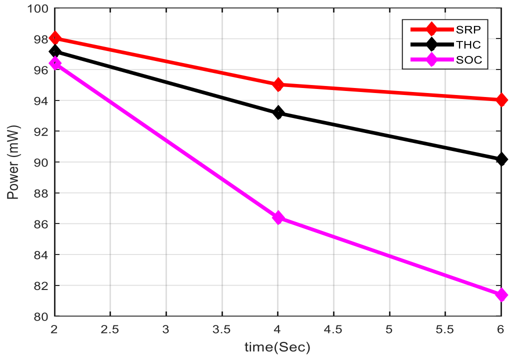

Fig.22: Power for varying packet size

Figure 21, 22 reveal the power consumption occurred on the application of proposed over a network. Here the network is a random in nature, i.e., the number of nodes is varying and also the packet size. Under both cases, the proposed approach shown the better performance compared with conventional approaches. With the increase in node density, the observed power consumption is comparatively increased due to higher security certificate exchange. However, the power consumption is observed to be lower for the proposed approach due to no requesting effort in certificate exchange in packet communication. This power saving impact on the node lifetime, which intern improves the network lifetime.

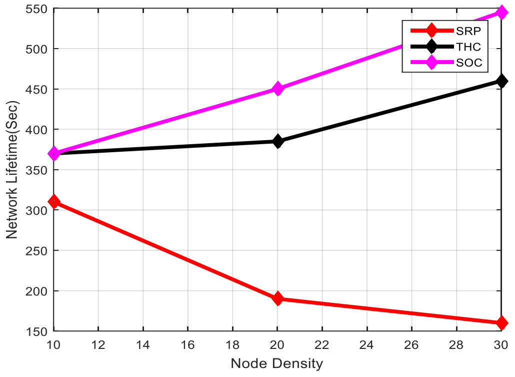

Fig.23: Network lifetime for varying packet size

Figures 23 reveal the performance of proposed approach with respect to the network lifetime under varying node density. With the increase in node density, the lifetime of the network improve due to lower packet exchange, the power required in forwarding the data is comparatively less in this case. The lower node switching result in lower power consumption in packet forwarding over a communication range. Thus, the proposed approach having better performance compared to THC and SRP.

V. CONCLUSIONZ

To develop a low overhead keying mechanism, a self monitored key mechanism is proposed. this mechanism overcome the issue of centralized monitoring. Centralized monitoring has the issue of high signaling overhead due to repetitive key requesting.

This leads to faster power draining and hence leads to network collapsing. In addition a key governance from a single centralized node leads to an issue of high reliability and the overhead on such node is very high due to large key repository and request accessing. In the suggested approach, this repository overhead is distributed among each user and the self repository creation and monitoring gives independent coding, eliminating the requesting overhead. This approach hence result in higher throughput and network life time in wireless adhoc network.

REFERENCES

1. Guanyu Tian ; Zhenhai Duan ; Todd Baumeister ; Yingfei Dong, "A Traceback Attack on Freenet", IEEE Transactions on Dependable and Secure Computing ,Volume: 14, Issue: 3, , pp-294 – 307, May-June 1 2017.
2. Xiaoxin Wu and Bharat Bhargava, "AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol", IEEE transactions on mobile computing, vol. 4, No. 4, July/august 2005.
3. Karim El Defrawy, and Gene Tsudik, "Privacy-Preserving Location-Based On-Demand Routing in MANETs", IEEE Journal On Selected Areas in Communications, Vol. 29, No. 10, December 2011.
4. Toby Xu, Ying Cai, "LSR: A Location Secure Routing Protocol for Ad Hoc Networks", Proc. IEEE Conf, 2010.
5. Nitesh Saxena, Gene Tsudik, and Jeong Hyun Yi, "Efficient Node Admission and Certificate less Secure Communication in Short-Lived MANETs", IEEE Transactions on Parallel And Distributed Systems, Vol. 20, No. 2, 2009.
6. Shushan Zhao, Robert D. Kent, Akshai Aggarwal, "An Integrated Key Management and Secure Routing Framework for Mobile Ad-hoc Networks", International Conference on Privacy, Security and Trust, 2012.
7. Hanan Saleet, Rami Langar, Otman Basir, and Raouf Boutaba, "A Distributed Approach for Location Lookup in Vehicular Ad Hoc Networks", IEEE ICC 2009.
8. R. S. Mangrulkar, Dr. Mohammad Atique, "Trust Based Secured Adhoc on Demand Distance Vector Routing Protocol for Mobile Adhoc Network", Proc. IEEE Conf, 2010.
9. Mohamed M. E. A. Mahmoud, Sanaa Taha, Jelena Misic, and Xuemin Shen, "Lightweight Privacy-Preserving and Secure Communication Protocol for Hybrid Ad Hoc Wireless Networks", IEEE Transactions on Parallel and Distributed Systems, IEEE, 2013.
10. Liu Yang, Markus Jakobsson, Susanne Wetzel, "Discount Anonymous on Demand Routing for Mobile Ad hoc Networks", Proc. IEEE, 2006.
11. Nitesh Saxena a, Gene Tsudik b, Jeong Hyun Yi, "Threshold cryptography in P2P and MANETs: The case of access control", Elsevier,2007.
12. M. Elena Renda, Giovanni Resta, and Paolo Santi, "Load Balancing Hashing in Geographic Hash Tables", IEEE Transactions on Parallel and Distributed Systems, Vol. 23, no. 8, August 2012.
13. Hanan Saleet, Rami Langar, Otman Basir, and Raouf Boutaba, "Proposal and Analysis of Region-based Location Service Management Protocol for VANETs", proceedings of IEEE "GLOBECOM", 2008.
14. Yan Lindsay Sun, Zhu Han, Wei Yuand K. J. Ray Liu, "A Trust Evaluation Framework in Distributed Networks: Vulnerability Analysis and Defense Against Attacks", in the proceeding of IEEE INFOCOM, 2006.
15. Pathak, D. Yao, and L. Iftode, "Securing Location Aware Services over VANET Using Geographical Secure Path Routing," Proc. IEEE Int'l Conf. Vehicular Electronics and safety (ICVES), 2008
16. Wei Yuan, "An Anonymous Routing Protocol with Authenticated Key Establishment in Wireless Ad Hoc Networks", International Journal of Distributed Sensor Networks, Volume 2014.
17. Yanchao Zhang, Wei Liu, Wenjing Lou, and Yuguang Fang, "MASK: Anonymous On-Demand Routing in Mobile Ad Hoc Networks", IEEE Transactions on Wireless Communications, Vol. 5, No. 9, September 2006.
18. Jun Long, Mianxiong Dong, Kaoru Ota, Anfeng Liu, "Achieving Source Location Privacy and Network Life-time Maximization through Tree-based Diversionary Routing in Wireless Sensor Networks", IEEE ACCESS, 2014.
19. Qiuna Niu, "Formal Analysis of Secure Routing Protocol for Ad Hoc Networks", IEEE, 2009.
20. S.M. Kamruzzaman, E. Kim, D.G. Jeong, W.S. Jeon, "Energy-aware routing protocol for cognitive radio ad hoc networks", IET Communications, 2012.
21. Haina Ye, Zhenhui Tan, Shaoyi Xu, Xiaoyu Qiao, "Load Balancing Routing in Cognitive Radio AdHoc Networks", IEEE, 2011.
22. Nitul Dutta, Hiren Kumar Dev Sarma, "A Routing Protocol for Cognitive Networks in presence of Co-Operative Primary User", IEEE, 2013.
23. Muhammad Zeeshan, Muhammad Fahad Manzoor, Junaid Qadir, "Backup Channel and Cooperative Channel Switching On-Demand Routing Protocol for Multi-Hop Cognitive Radio Ad Hoc Networks (BCCCS)", ICET, 2010.
24. Alexander W. Min, and Kang G. Shin, "Robust Tracking of Small-Scale Mobile Primary User in Cognitive Radio Networks", IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No. 4, April 2013.
25. R.Vadivel, V. Murali Bhaskaran, "Energy Efficient With Secured Reliable Routing Protocol (EESRRP) For Mobile Ad-Hoc Networks, Procedia Technology, Elsevier, 2012.
26. Abu TahaZamani, "A Novel Approach to Security in Mobile Ad HocNetworks (MANETs)", International Journal of Computer Science and Information Technology Research Vol. 2, Issue 1, pp: (8-17), Month: January-March 2014.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)