PROVISIONING OF EFFICIENT AUTHENTICATION TECHNIQUE FOR IMPLEMENTING IN LARGE SCALE NETWORKS (PEAT)

S. Lingeshwari
PG Scholar, Department of CSE, PSN Engineering College, Tirunelveli
Email: lingeshwarii@gmail.com

R. Natchadalingam
Associate Professor, Department of CSE, PSN Engineering College, Tirunelveli

Abstract--- Increasing attractiveness of Ad-hoc Networks, its quality and treatment has guide in the introduction of threats and attacks to bring negative consequences in the society. The typical features of ad hoc network, particularly with dynamic topology and open wireless medium, may lead network afflicted with some refuge vulnerabilities. The main challenge in designing an ad hoc network is to build them protective from different attacks in the network. The authentication must be done without much delay and should independent of the other packets. In this system we propose, Provisioning of Efficient Authentication Technique for Implementing in Large Scale Networks (PEAT). Here the Clusters are formed based on the distance and the Cluster Heads (CHs) are elected by coverage and connectivity. The secret key generation used to form the clusters securely. The CH first checks the cluster members’ secret key then formed the clusters. The Elliptical Curve Cryptography technique verifies the CH is authenticated or not. Hence, source sends the data to authenticated CH in the network. Simulation results shows that the PEAT perform better amount of data received also reduce the delay in the network.

Keywords**—**Secret key Management, Elliptical Curve Cryptography technique, Wireless Sensor Network.

1. Introduction

In recent years, ad hoc networks have concerned much attention in the wireless investigate engineering community motivated by applications such as asset tracking, battlefield, situational awareness, air-borne safety and border protection [1]. This network applications is significant to devise competent network management solutions suitable for nodes that are constrained in onboard energy and in their computation and transmission capacities. In addition, the solutions must be scalable to support networks covering vast areas with a large set of nodes that communicate over many hops. These characteristics make the design and management of ad-hoc networks significantly challenging in comparison to contemporary networks. In particular the provided network services need to achieve the following security goals: (1) Confidentiality, to avoid opponents from reading communicated data, (2) Message integrity, to avoid tampering with transmitted messages, and (3) Source Authentication, to protect man-in-the-middle attacks that may replay transmitted data for no deimpersonation. Confidentiality is achieved by encrypting the transmitted data. Clustering is a standard approach for achieving well-organized and scalable performance in wireless networks. Clustering facilitates the distribution of control over the network, and hence, enables locality of communication. Moreover, clustering nodes into groups saves energy and reduces network contention as nodes communicate their data over shorter distances to their respective CH. The work presented in this paper aims at addressing the unauthenticated nodes in the network. The ECC key is used to identified the unauthenticated nodes and secret key is used to form the secure clusters in the network.

The paper is organized as follows. The next section treats the related work. In Section III, the proposed system Provisioning of Efficient Authentication Technique for Implementing in Large Scale Networks (PEAT) is described. Section IV analyzes the performance of PEAT. Finally, Section V concludes the paper.

2. Related Work

Tiered Authentication of Multicast Protocol for Ad-Hoc Networks (TAM) [1] introduced network clustering to reduce overhead and ensure scalability. To authenticate the message source one-way hash chains is used within the same cluster. To authenticate the source each cluster looks for a distinct combination of MACs in the message. While establishing the multicast session, the source starts generates the keys. Then keys will be securely transmitted to the head of each clusters. The advantages of the TAM are secret information asymmetry and the time symmetry paradigms. Secure clustering and symmetric key establishment in heterogeneous WSNs [2] consist of pairing-based secure key management scheme. A multiuser broadcast authentication is presented that emphasizes the use of public key cryptography in heterogeneous WSNs. It is applicable for special kind of WSNs with many user nodes. The scheme all messages broadcasted from the gateways should be authenticated. Therefore, the messages from illegitimate users or compromised sensor nodes can be easily rejected by the other nodes.

A Hierarchical Identity Based Key Management Scheme [3] explained distributed hierarchical key management scheme to select the best nodes to function as the PKG taking into account the nodes security conditions and energy states. This scheme improves the network security and maximizing the network lifetime.

Overlapping Multi hop Clustering for WSNs [4] to minimizing the energy spent in communicating the information to the processing center. The NP-hard introduced the KOCA randomized multi-hop heuristic algorithm that generates connected overlapping clusters covering the entire sensor network with a specific average overlapping degree. KOCA provides high network coverage and connectivity. It controls the cluster size. Location-Aware Combinatorial Key Management Scheme [5] used to balance security and efficiency by using small-size hints and batch rekeying, respectively. The solution minimizes the energy and memory consumption of the security protocol through trading off the number of keys and rekeying messages. A major drawback that hampers the use of most of these group key management protocols in WSNs is the lack of support for faulty and misbehaving nodes, and the overhead incurred to support key management activities including setup and rekeying.

Talking To Strangers: Authentication in Ad-Hoc Wireless Networks [6] presented new schemes for peer-to-peer authentication. in ad-hoc wireless networks. It provides the user with an extremely intuitive way to identify and authenticate parties to a communication. This scheme does not require a public key infrastructure, and do away with the naming problem that plagues traditional authentication systems. The BiBa one-time signature and broadcast authentication Protocol [7] explained the BiBa signature. This signature scheme immediately yields important new applications. In particular, it extend the BiBa signature scheme to design a new protocol for authenticating broadcasts, such as streaming information broadcast over the Internet. Many applications need to authenticate broadcast data, i.e. verify the data origin. Efficient Authentication and signing of multicast streams over lossy channels [8] presents two very different solutions to the problem of authenticating data streams efficiently in a lossy environment. The first solution, called TESLA (for Timed Efficient Stream Loss-tolerant Authentication), uses only symmetric cryptographic primitives such as pseudorandom functions (PRFs) and message authentication codes (MACs), and is based on timed release of keys by the sender.

An authentication service based on trust [9] introduced secure, scalable, and distributed authentication service that enhances the correctness of public key certification. The trust model allows nodes to monitor and update trust values for each other in a distributed manner. The network model is clustering-based; this facilitates behavior monitoring and provides high availability for public key certification. It provides security operations, including public key certification, identification and isolation of malicious nodes, and trust value update in a novel way.

3. Proposed Method

An Ad hoc network is a collection of autonomous nodes that together set up a topology without the support of a physical networking infrastructure. Depending on the applications, a sensor network may include up to a few hundreds or even a thousand nodes. In this system, the nodes are grouped into clusters. The clusters are formed based on location. The Cluster Head (CH) controls every cluster. The CH is elected based on the node coverage and connectivity. Every cluster member communicates another node through a CH. Fig. 1. Illustrate the architecture of the proposed scheme.

In this protocol, The key distribution phase broadcast the secret key to cluster members. Before the cluster formation, the CHs check the cluster members secret key. The secret key computation is given below.

$$SK_i = \sum_{i=1}^{h} (y_i)(x_i - x_{CH}) \qquad (1)$$

Where

h→Number of cluster members

x_i → x position of cluster member

$y_i \rightarrow y$ position of cluster member

$x_j \rightarrow$ position of CH

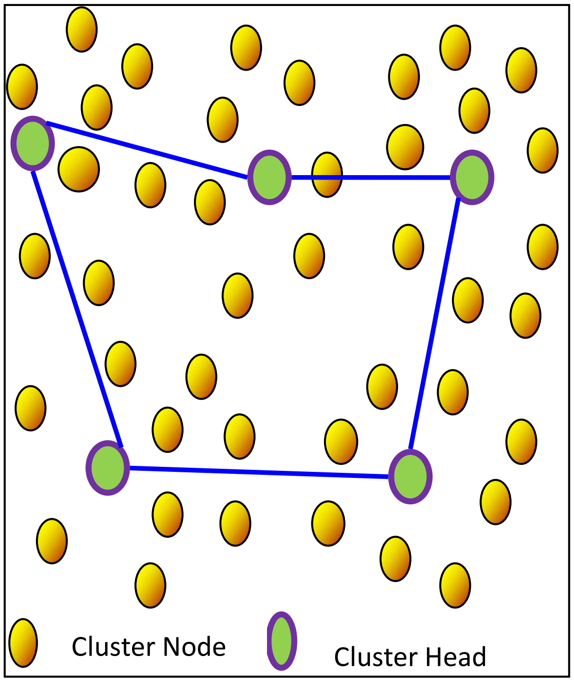

Fig: 1 Architecture diagram

If a source wants to communicate the data to destination, it first sends the data to its CH. The CH checks the source secret key. If the key is match then it sends the data to next CH. Then the CH is verified based on the Elliptical Curve Cryptography technique. If the CH is authenticated then the source send the message otherwise it send notification message to all nodes and isolate the unauthenticated CH. This process is continued until the source reaches the destination. Hence, the source transmits the data to reliable nodes in the networks.

The Elliptical Curve Cryptography key generation is given below.

$$l + m = n \quad \text{Where } l \neq m \text{ and } \forall l, m \in E \qquad (2)$$

Where (x_l, y_l) and (x_m, y_m) and (x_n, y_n) are the coordinates of the l, m and n. The co-ordinates (x_n, y_n) can be obtained by,

$$x_n = \gamma^2 - x_l - x_m \qquad (3)$$

$$y_n = \gamma(x_l - x_n) - y_l \qquad (4)$$

where, $\gamma = \dfrac{y_m - y_l}{x_m - x_l}$

The commutative property of this function states that,

$$l + m = m + n \quad (5)$$

The L_{sk} and R_{sk} is given below

$$L_{sk} = l + m \quad (6)$$

$$R_{sk} = m + n \quad (7)$$

The source compares its L_{sk} with the R_{sk} , if it equal the source send the data to another CH otherwise the source published the CH is unauthenticated.

4. Performance Evaluation

In this section, we analyze the simulation results of proposed method. The performance evaluation is done through the Network Simulator ns-2. In this simulation, 60 nodes randomly distributed within the network field of size 1400m×1400m. The parameters used for the simulation of the RAF-EERM are tabulated in table1.

Table 1. Simulation parameters of RAF-EERM

Parameter	Value
Simulation Area	1400 x 1400m
Number of Nodes	60
Channel	WirelessPhy
Channel Data Rate	10 Mbps
Radio Propagation Model	TwoRayGround
Antenna Type	Omni Antenna
Traffic Models	CBR/TCP
CBR Interval	1.0 ms
Communication Model	UDP
Mobility Model	Random Way Point
Simulation Time	100

The traffic is handled using the traffic model CBR. The radio waves are propagated by using the propagation model two ray ground. All the nodes receive the signal from all direction by using the Omni directional antenna. The performance of the PEAT is evaluated by the parameters packet delivery rate, packet loss rate, average delay, throughput and residual energy.

Packet Delivery Rate:

Packet Delivery Rate (PDR) is the ratio of amount of data packets established to the amount of data packets sent by the source node. The PDR is calculated by the equation (8). The figure 2 reports that the amount of data packets received by the PEAT is larger than the TAM.

$$PDR = \frac{Total\ Pack\ Received}{Total\ Pack\ Send} \tag{8}$$

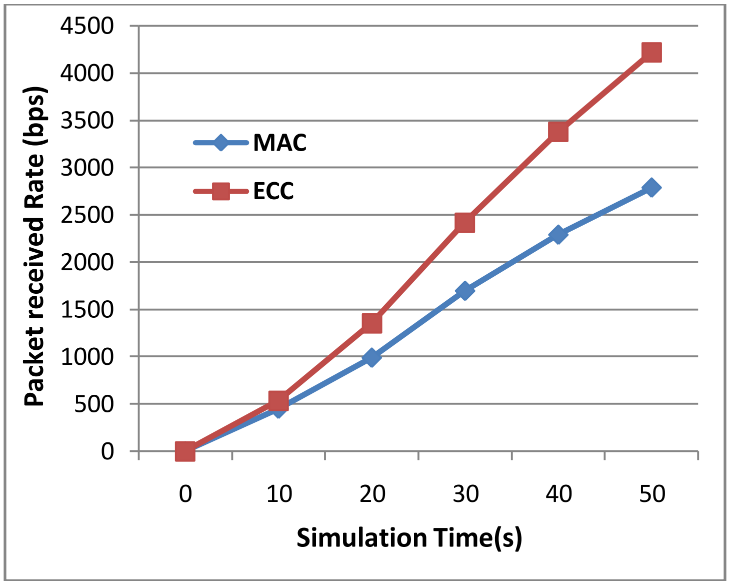

Fig. 2 Packet Delivery Rate of MAC and ECC

Packet Loss Rate:

The Packet Loss Rate (PLR) is the ratio of the number of packets dropped to the number of data packets sent. The PLR is calculated by Equation (9).

$$PLR = \frac{Total\ Pack\ Dropped}{Total\ Pack\ Send} \tag{9}$$

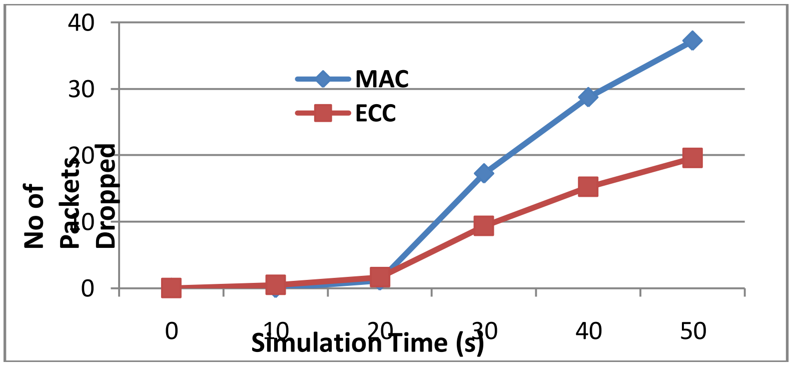

Fig. 3 Packet Loss Rate of MAC and ECC

The figure 3 shows the packet loss rate of the PEAT protocol is lesser than that of the TAM protocol showing the efficiency of the PEAT.

Average Delay:

The average delay is defined as the time difference between the current packets received and the previous packet received. It is measured by Equation (10).

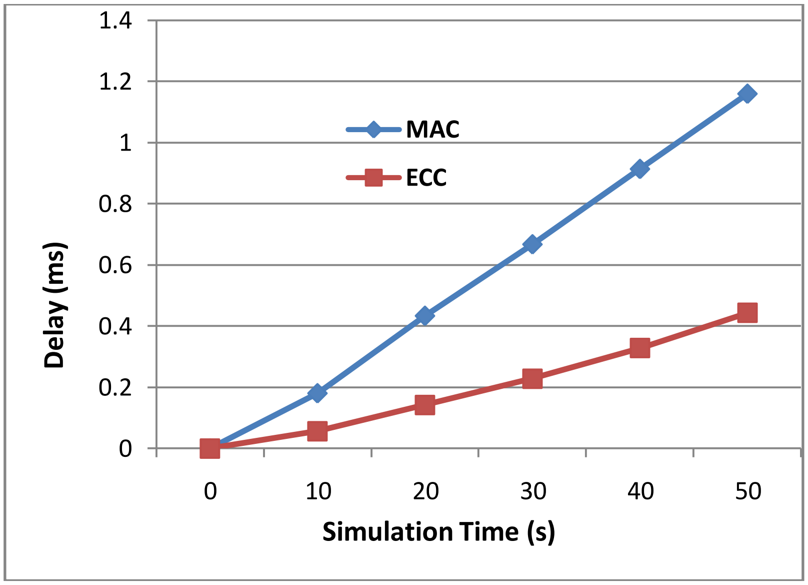

Fig. 4 Delay of PEAT and TAM

$$Average\,Delay = \frac{Pack\,Recvd\,Time - Pack\,Sent\,Time}{time} \qquad (10)$$

Figure 4 demonstrate that the delay of PEAT and TAM. The average delay of the TAM is larger than the PEAT indicating the improved performance of the PEAT protocol.

Throughput:

Throughput is the average of successful messages delivered to the destination. The average throughput is calculated using Equation (11).

$$Throughput = \frac{\sum_0^n Pack\,Received\,(n) * Pack\,Size}{1000} \qquad (11)$$

The figure 5 shows the performance of throughput of PEAT and TAM protocols. The throughput of the TAM is lesser than the PEAT. It represents increase the efficiency of the PEAT protocol in the network.

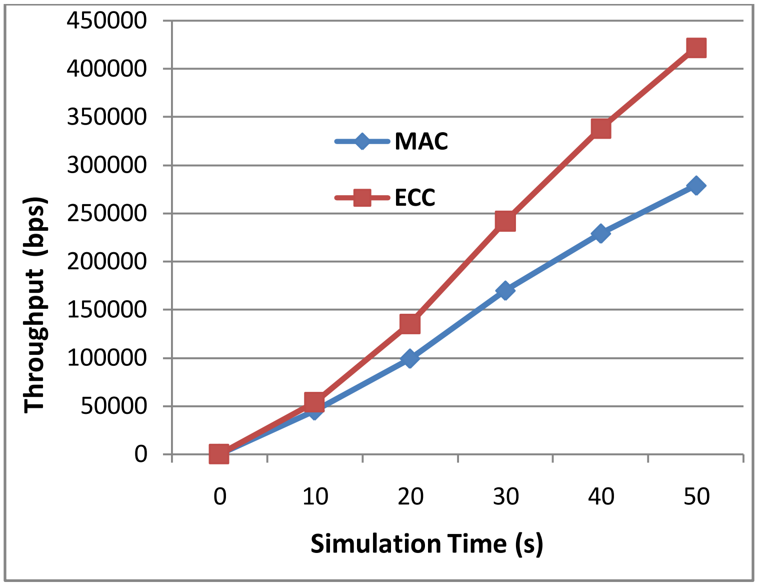

Fig.5 Throughput of TAM and PEAT

5. Conclusion

Provisioning of Efficient Authentication Technique for Implementing in Large Scale Networks (PEAT) is proposed in this paper. Here the Clusters are formed based on the distance and the Cluster Heads (CHs) are elected by connectivity. Before cluster formation, the CH checks the cluster members by secret key generation. This secret key is used to form the clusters securely. The Elliptical Curve Cryptography technique is verified the CH is authenticated or not. Therefore, it offers data to trusted CH in the network. The simulation results shows that the PEAT perform better amount of data received also reduce the delay in the network.

REFERENCES

[1] Younis, M.,"TAM: A Tiered Authentication of Multicast Protocol for Ad-Hoc Networks" IEEE Transactions On Network And Service Management, Vol. 9, No. 1, March 2012 .

[2] Azarderskhsh, R., and Masoleh, A., "Secure clustering and symmetric Key establishment in heterogeneous wireless sensor networks," EURASIP J. Wireless Commun. Netw., vol. 2011, 2011.

[3] Yu, F.R, Tang, H., Mason, P., and Wang, F.," A hierarchical identity based key management scheme in tactical mobile ad hoc networks," IEEE Trans. Netw. Service Management,vol. 7, no. 4, pp. 258-267,Dec. 2010.

[4] Toussef, M., Youssef, A., and Younis, M.," Overlapping multihop clustering for wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 12, pp. 1844-1856, Dec. 2009.

[5] Younis, M., Ghumman, K., and Eltoweissy, M.," Location-Aware Combinatorial Key Management Scheme for Clustered Sensor Networks," IEEE Trans. Parallel Distrib. Syst., vol. 17, no. 18, pp.865-882, Aug. 2006.

[6] Ngai E.C.H., and Lyu, M.R.," An Authentication service based on trust and clustering in wireless ad hoc networks : description and security evaluation ," in Proc. 2006 IEEE International Conf. Sensor Networks, Ubiquitous,Trustworthy Computing.
[7] Perrig, A., "The Biba one-time signature and broadcast authentication protocol," in Proc. 2001 ACM Conf. Computer Commum. Security.
[8] Reyzin, L., and Reyzin, N., "Better than Biba: short one-time signatures with fast signing and verifying," in Proc. 2002 Australian Conf. Info. Security Privacy, pp. 144-153.
[9] Perrig,A., Canetti, R., Tygar, J.D., Berkely, UC., Fountain, D., Watson, T.J., " Efficient and secure source authentication for multicast," in Proc. 2001 Network Distributed System Security Symposium.