ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 11, November 2016

A Trust-Aware Routing Framework with Hop-by-Hop Authentication in Wireless Sensor Networks

[1]Krishna Murthy [2]Dr. C. Shoba Bindu
[1]PG Student, [2] Professor
Department of Computer Science and Engineering
Jawaharlal Nehru Technological University, Anantapur India

***Abstract:* -- The advancements in the Wireless technology activate the wireless users, to obtain its services with resource constraints.Due to the constraints in transmission range, multiple counts of 'hops' are needed to build a network to efficiently transfer the data across the networks. Therefore, the multi-hop networks should be protected from any external or internal attackers. The data should be delivered at the receiver end,without any modification. In order to protect the data from any intruders, we build trust aware routing protocol systems.We propose a trusted framework for hop-by-hop authentication scheme in wireless sensor networks. The objective of the study is to significantly reduce the data modification rate from the attackers. In addition to, a scalable Elliptic Curve Cryptography (ECC) is studied to establish an effective authentication process. By doing so, the data transmission between sender and receiver is effective, without considering the threshold issue. It supports for better decision making process.Both conceptual analysis and parallel results demonstrate that our proposed scheme is more efficient than existing works.**

***Keywords:*-- Hop-by-hop authentication, Wireless sensor networks, trust management, Secure routing and Elliptic Curve Cryptography (ECC)..**

I. INTRODUCTION

With the greater developments in Wireless Sensor Networks (WSN) in the field of battle, military applications and in some sensitive applications, plays an irresistible role among the wireless users.In a short communication range, the multi-hop path is formed by the information sensed by sensor nodes from base station [1]. In doing so, there is a higher chance of malicious activities, to be performed in Multi-hop routing process. The intruders can tamper the nodes, generating traffic among the sensor nodes, dislocate or drop the routes and also pose some interference among the sensor nodes [2].This paper concentrates on the replaying attacks.Depending upon the receiver's identity, the routing information gets modified by the intruders. They can also impose the attacks like wormhole and sinkhole attacks [3]. It, tremendously, replays all the routing information transformation between sender and receiver node. The packet that holds original headers are replayed. In direct transmission system, the malicious user finds tricky, to collide the nodes, thus in this case, the routing packets are replayed. This type of attacks is known as wormhole attacks. The packets are mainly used for the recognizing the identity of the sender. By stealing the sender's identity, the intruders create network traffic.

In the selective forwarding attack scenario, the packets are dropped by the intruders. Here also, the prediction of the delivery of the received packets to the intended receivers is hard, using the overhearing schemes [4]. Similarly, the sinkhole attacks are not easy to use in real time applications.The malicious node may acts as base station, to perform replay attacks. This is further enhanced by creating traffic, which is yelled out as 'black hole attacks'.

In previous works, the intention of the routing protocols is to maximize the node's efficiency by the lessened rate of energy consumption,and also, to enhance the participation of the authorized users.Security is the important aspects of the wireless users. By the better use of routing information, malicious node can't participate in the network, even in case of valid node's identity.

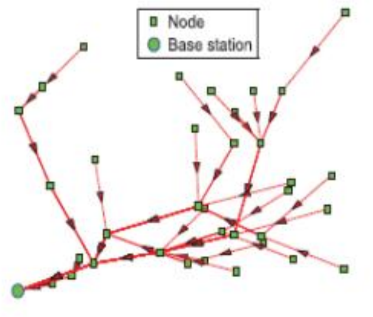


Fig .1 Multi-hop routing for data collection of a WSN

This can be further enhanced by the introducing the concept of Mobility in WSN.When the network connection is slow, the differentiation between intruder and normal user is trickier [3]. The nodes with improper security schemes may suffer from all sorts of attacks. Energy efficient is also an important parameter for the battery typed sensor nodes under various topological. Randomization of the nodes is used for forwarding the packets [4]. In extension to this, some cryptographic methods are used for building the trust and reputation oriented systems in order to secure the networks. Secure routing solutions based on trustand reputation management rarely address the identity deception through replaying routinginformation [5].

The rest of the paper is organized as follows: Section II describes about the existing works carried out by other researchers; Section III presents the role of proposed system; Section IV validates the proposed works through some experimental model. At last, concludes in Section V.

II. LITERATURE SURVEY

This section explains about the previous works carried out by other researchers. We presenttrust-aware routing protocols in the wireless sensor networks. Xiaoqi et al presented the trusted AODV protocol [7]. It is further enhanced from the traditional AODV protocol systems. The various trust oriented metrics are studied. The decision rules are created by the AODV systems. The trust models are introduced to the information exchange process. It includes three process namely, route table extension, message extension and trusted recovery process.

This was further extended to the dynamic routing. The Dynamic Source Routing (DSR) protocol is studied by including 'watch dog' and 'Pathrater' mechanisms [8]. The role of the watchdog system is to discover the nodes, which fail to coordinate with the networks. By doing so, the transmitted packets are buffered for a while in the networks. Next, the role of Pathrater is to schedule the nodes according to the feedback from its neighboring nodes. The ratings are given to the most frequently selected routes by the source nodes. It is studied by Pirzada et al [9].

The trust cum confidentiality of the data and nodes are studied by the authors in [10]. CONFIDANT is abbreviated as 'Cooperation of Nodes, Fairness In Dynamic Adhoc NeTworks. It assists the Watchdog and Pathrater scheme, by acting as Trust Manager. The purpose of trust manager is to monitor the network events by watchdog mechanism. An alarm signal is forwarded to the nodes, if the manager detects any unsuspicious events. It is maintained as 'friends list' of the authentication mechanism. Similarly, the reputation system maintains the list of black nodes and mutually shares between the nodes.The similar scheme is further extended and proposed as CORE [11]. The unique feature is that CORE fragments into three parts, namely, Subjective reputation, Indirect reputation and functional reputation. Subjective Reputation, which is observed through own observations; Indirect Reputation, which is a positive report by another node; and Functional Reputation, which is based upon behaviour monitored during a specific task. Based on these, a reputation value is obtained for securing the networks.

The routing protocol was further extended to the Greedy Perimeter Stateless Protocols (GPSR), which calibrates the trust levels. Depending on the time constraints, the packets are forwarded to the packets. Thus, the trust value is estimated for its neighboring state. It is improved by considering decisions systems and it is coined as Trust Routing for Location aware Sensor Networks (TRANS). It selects routes based on the estimated trust value [11]. In this, the sink forwards the packets to its neighbors.

A security oriented trusted protocols is known as'SPINS' [12]. It supports confidentially, data authentication and the freshness of the data. It comprised of two blocks namely, SNEP and µTESLA. It doesn't holds any counter values instead it achieve semantic oriented security. The role of µTESLA[13] is to enhance the authentication between the nodes. But it fails to focus, DOS attacks. Ariadne [14] is efficient, using only highly efficient symmetric cryptographicprimitives and uses per-hop hashing functions. It also assumes the use of TESLA and MACauthentication mechanisms.

III. PROPOSED SYSTEM

3.1 Issues

As previous works, a secure and efficient SAMA scheme is introduced. The main thought of this scheme is to secure the data. It is done by elliptic curve model. For a ring signature, each ring member is required to compute a forgery signature for all other members in the AS.The entire SAMA generation requires only three steps, which link all non-senders and the message sender to the SAMA alike. In addition, our design enables the SAMA to be verified through a single equation without individually verifying the signatures. As it lacks in terms of packet delivery ratio, packet loss and routing overhead, the proposed trust aware routing framework in hop-by hop authentication is modelled, to resolve the issues arises in terms of trust metrics.

3.2 Trust aware Routing protocols

In order to overcome the replay routing information attacks, we design a trust aware routing protocols using hop-by-hop authentication scheme. The fig.2 presents the system model.

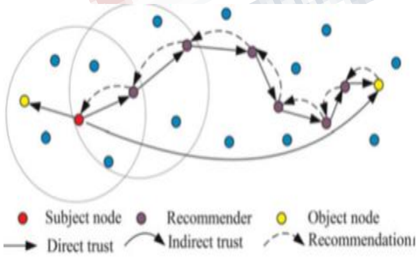


Fig.2 System Model

The proposed system model comprised of two actors, namely, Energy Watcher and Trust Manager.

i) Energy Watcher

Energy watcher estimates the cost of the energy from its neighbour's node information. It, distinctly, maintain the neighbourhood table that consist of neighboring nodes and its estimated costs ENb. The ENb is defined as the mean cost of delivered packets from source to destination via base station, and b as the next-hop node. Relied upon the threshold level, packets transmission among the nodes is defined. The packet transmission is decided on the energy cost and trust value.

ii) Trust Manager

Trust manager performs its role on certain constraints,

i) The node N will execute in the loop for few iteration. If it detects the low trust value, then the next hop node is selected for communication.
ii) In certain cases, the node N can't detect the next hop node, and then the communication link gets broken.

The trust manager checks the nodes for traffic creation. It equalizes the stored value of <source node id, intervals [a, b] with significant length>. Let us consider a node N, which contains one-hop wireless transmission. The trust value is ranged from [0,1]. The probability between base station and the neighboring node n is computed for assigning the trust level of a node. Let T be the trust value and E is the energy cost. It quantifies link quality estimation in order to choose a next-hop node.

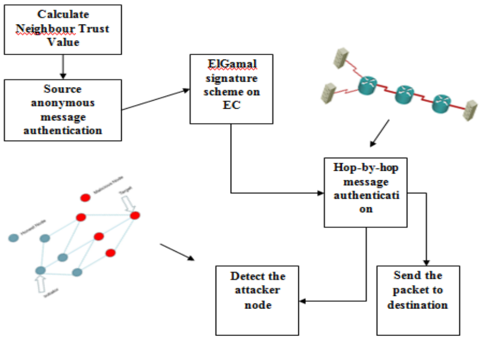

Calculate Neighbour Trust Value
Source anonymous message authentication
ElGamal signature scheme on EC
Hop-by-hop message authenticati on
Detect the attacker node
Send the packet to destination

Fig.3 Proposed System

a. Modules

The modules for trust-aware routing framework with hop-by-hop authentication are listed as follows:

A. Network Configuration
B. Direct Rust
C. Recommendation Trust
D. Source Anonymous Message Authentication
E. Hop By Hop Message Authentication

3.2.1.1 Network Configuration

The sensor nodes are deployed randomly in the wireless sensor environments. The nodes are stationary. The information is sensed by the sensor nodes via base station. By the use of intermediate node,the packet transmission is done.

3.2.1.2 Direct Trust

The task of direct trust is to derive the trust value and quantification of the nodes. Let x and y be two nodes in the wireless communication medium. It is generalized as follows:

$$D_t(x, y) = \frac{p_s}{p_r} \qquad (1)$$

The above eqn. (1) is used for estimating the trust value between node x and node y, where D_t (x, y) possess the final trust value of x and y; $p_s$is the success rate of the sent packets from node x and p_r is the success rate of the received packets to node y.

3.2.1.3 Recommendation Trust

The purpose of the recommendation trust is to acquire the information from neighboring nodes related to the trust values. In order to eliminate the risk of bad mouthing attacks, the direct trust value estimation is recommended. It is yelled out as 'recommendation trust'.

It is performed as follows:

- ♣ Node X sends RTREQ to node(s) N.
- ♣ If node X has direct trust value on Y, then it will reply back with RTREP.
- ♣ Else If X does not have direct trust value record it will discard the RTREQ
- ♣ After receiving RTREP reply from neighbours consider the trust value of the node with maximum direct trust value by applying fuzzy logic.
- ♣ Integrate all the obtained RT value from neighbours to calculate the indirect trust value.
- ♣ Atlast, the node which possess higher trust value is recommended.

3.2.1.4 Source Anonymous Message Authentication (SAMA)

The previous SAMA scheme is incorporated to enhance the message authentication scheme. It mainly used for transmitting the packets in secured fashion. It doesn't restrict the nodes by threshold issue. And the security is further enhanced by ElGamal Signature scheme.It removes the corrupted messages by authentication mechanism. Then the SAMA code is generated using elliptic curve form, to find the source anonymity.

3.2.1.5 Hop-By-Hop Message Authentication

The data is being protected by the hop-by-hop message authentication system.Each packet is embedded with the signature, to avoid the activities of the adversaries. It also ensures whether the message is modified or not. If the forwarder detects any malicious events, then the packet is dropped or the routing path is altered.

IV. PERFORMANCE EVALUATION

4.1 Simulation Parameters

The proposed model is experimented using NS2 tool [16]. The network standard of IEEE 802.11 [17] MAC with a channel data rate of 11 Mb/s.It is tested with two evaluation metrics such as number of deviated nodes, number of nodes in the MAC layer and the mean number of bits transmitted between source and destination.

4.2Simulation Results

The performance evaluation of the proposed model is defined as follows:

a) **Packet Delivery Ratio (PDR):** The rate of packets delivered at the receiver side to the rate of packets send from the source end.

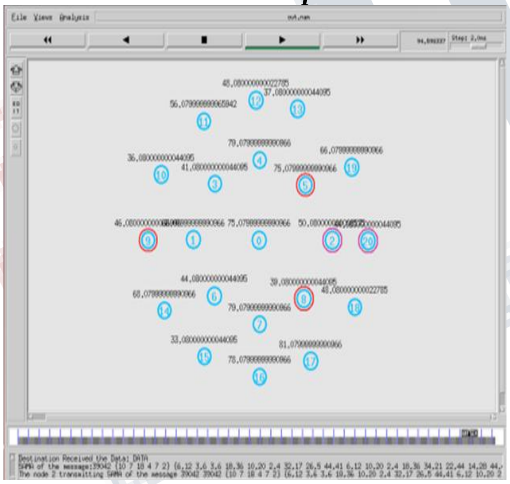
b) **Delay:** Delay is the time estimated for the packets travelledfrom source to destination

c) **Packet Loss**: It is defined as the total number of packet lost while transmitting from source to destination node.

A graph is plotted between time and packet size to study the delay in the proposed system and is shown in Fig. 5, packet delivery ratio and in fig .6, packet loss and finally fig.7 end to end delay. Thus result shows that proposed system is efficient than the existing system.

Parameter	Value
Application Traffic	10 CBR
Transmission rate	4 packets/s
Packet Size	512 bytes
Channel data rate	11 Mbps
Area	700m*700m
Simulation time	800

Table 1. Simulation parameters



```
Destination Received the Data: DATA
SAMA of the message:39042 (10 7 18 4 7 2) (6.12 3.6 3.6 18.36 10.20 2.4 32.17 26.5 44.41 6.12 10.20 2.4 18.36 34.21 22.44 14.28 44.
The node 2 transmitting SAMA of the message 39042 39042 (10 7 18 4 7 2) (6.12 3.6 3.6 18.36 10.20 2.4 32.17 26.5 44.41 6.12 10.20 2
```

Fig .4 TARP with Hop by Hop Message Authentication

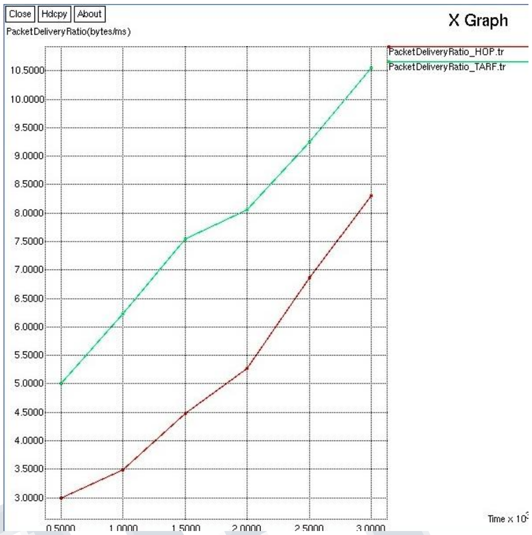


Fig .5Packet Delivery Ratio

This graph shows that the packet delivery ratio of the proposed system is high when compared with that of existing system because in this there is no congestion in the network traffic which increases the delivery of packets that are being sent.

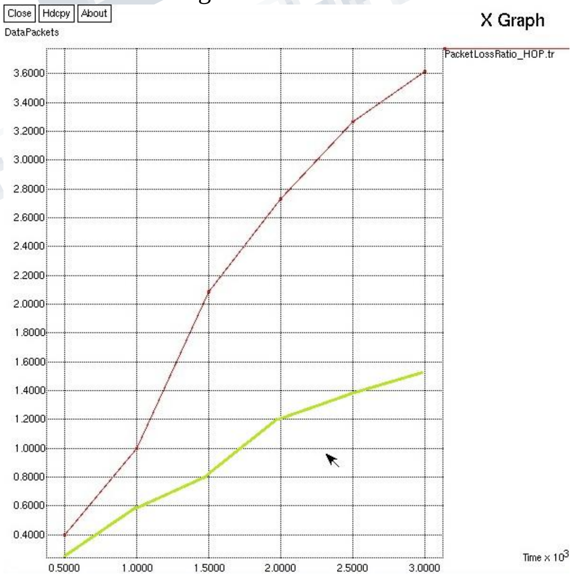


Fig.6 Packet Loss

This graph shows that the packet delivery ratio of the proposed system is high when compared with that of existing system because in this we considered the energy and trust watcher which concentrates on increasing the energy of the nodes and also the trust worthiness of neighbouring nodes that minimises the packet loss.

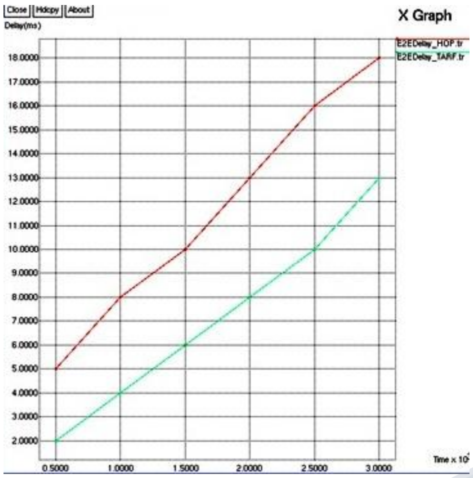


Fig.7 End to End delay

Above graph shows the variation of the delay.HOP by hop consistently shows the highest delay. Tarf with Hop by hop has the lowest delay as compared to the Hop by Hop. One factor can be that it have less throughput (Number of packets delivered per unit time) so it is having the less delay

V. CONCLUSION

This paper intends to study about the trust aware routing protocols in Wireless Sensor Networks (WSN). We propose a hop-by-hop authentication message system that significantly reduces the tasks of malicious node. A trust value is obtained for every node in the wireless networks. Relied upon the trust value, the routing path is determined. The trust is estimated in two forms: a) Direct trust and b) Recommendation trust. An adversary model is designed, so as to study about the normal and abnormal nodes. By the advent of SAMA scheme, the packets are verified and transmitted to the receiver. The receiver node can also check whether packets get modified or not. Experimental analysis is done using NS2 tool, in terms of performance metrics such as Packet delivery ratio, Packet loss and End-to End delay. By doing so, the packet dropping is reduced, so as to achieve accurate trusted network.

REFERENCES

[1] Ji Guo , Alan Marshall, Bosheng Zhou, “A New Trust Management Framework for Detecting Malicious and Selfish Behaviour for Mobile Ad hoc Networks”, International Joint Conference of IEEE, 2011.

[2] Manoj V, Mohammed Aaqib ,Raghavendiran N and Vijayan R “A Novel Security Framework Using Trust and Fuzzy Logic in MANET”, International Journal of Distributed and Parallel Systems (IJDPS), 2012.

[3] Jaydip Sen, “A Survey on Reputation and Trust-Based Systems for Wireless Communication Networks”, Computer Research Repository of IEEE, 2010.

[4] Vijayan R, Mareeswari V and Ramakrishna K, “Energy based Trust solution for Detecting Selfish Nodes in MANET using Fuzzy logic”, International Journal of Research and Reviews in Computer Science (IJRRCS), 2011

[5] Yacine Rebahi, Vicente .E Mujica-V and Dorgham Sisalem, “A Reputation-Based Trust Mechanism for Ad hoc Networks”, Proceedings of IEEE symposium on computers and communications, 2005.

[6] Sonja Buchegger, Jean-Yves Le Boudec, “A Robust Reputation System for Mobile Ad-hoc Networks”, EPFL IC Technical report IC, 2003.

[7] Ramprasad Kumawat and Vinay Somani “Comparative Study of On -demand Routing Protocols for Mobile Ad-hoc Network”, International Journal of Computer Applications,2011.

[8] Hui Xiaa, Zhiping Jiaa, Xin Lia, Lei Jua, Edwin H.-M. Shab, “Trust prediction and trust-based source routing in mobile ad hoc networks”, ScienceDirect Ad hoc Networks , 2010.

[9] Pankaj Sharma and Yogendra Kumar Jain,”TRUST based Secure AODV in MANET”, Journal of Global Research in Computer Science, 2012.

[10] Rajan Shankaran, Vijay Varadharajan, Mehmet A. Orgun, and Michael Hitchens, “Critical Issues in Trust

Management for Mobile AdHoc Networks", IEEE Information Reuse and Integration, 2009.

[11] G.S. Mamatha, Dr. S.C. Sharma, "Network Layer Attacks and Defense Mechanisms in MANETS- A Survey", International Journal of Computer Applications, 2010

[12] Imrich Chlamtac, Marco Conti, Jennifer J.-N. Liu, "Mobile ad hoc networking: imperatives and challenges", ScienceDirect Ad Hoc Networks, 2003.

[12] T.A. ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Trans. Information Theory, 1985.

[13] H. Wang, S. Sheng, C. Tan, and Q. Li, "Comparing Symmetric-Key and Public-Key Based Security Schemes in Sensor Networks: A Case Study of User Access Control," Proc. IEEE 28th Int'l Conf. Distributed Computing Systems (ICDCS), 2008.

[14] D. Pointcheval and J. Stern, "Security Proofs for Signature Schemes," Proc. Advances in Cryptology (EUROCRYPT), 1996.

[15] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," Comm. ACM, 1981.