International Journal of Engineering Research and Reviews ISSN 2348-697X (Online)
Vol. 3, Issue 3, pp: (96-101), Month: July - September 2015, Available at: www.researchpublish.com

An Adaptive QoS Strategy Based on Trust to Secure Multi-Hop Routing in Wireless Sensor Networks

[1]Asha S., [2]Devi Murali

[1]PG Scholar, Assistant Professor,

Department of Communication Engineering, Sree Buddha College of Engineering for Women, Elavumthitta, Pathanamthitta, India

Abstract: **Wireless Sensor Network has a huge scope in research and many application areas but sensor networks are vulnerable to different attacks. So to protect these sensor networks from various advisories message authentication with security is a perfect solution. Thus by considering this factor many authentication schemes have been developed, based on either symmetric-key cryptosystems or public-key cryptosystems. But many of these schemes have the restrictions of high computational overhead and lack of scalability. So as a solution to this problem a scalable authentication scheme based on elliptic curve cryptography (ECC) along with a trust model has been introduced. This work enables intermediate nodes authentication to secure the wireless sensor network and to regularize the multi-hop routing techniques. This scheme can provide energy-efficient routing and reliable trust and good packet delivery ratio. This routing technique can also act as an effective solution against harmful attacks.**

Keywords: **Message Authentication, Security, Trust wireless sensor networks and Routing.**

I. INTRODUCTION

Wireless Sensor Networks are a type of Adhoc networks with wirelessly interconnected sensor nodes. Sensor nodes may perform the function of sensing, data relaying, and data exchanging with other networks outside the WSNs. The issue of secure routing in wireless is a major challenging design factor in different networking aspects. And the problem gets more complicated when infrastructure-less networks that exhibit even more constraints and new types of attacks are considered. Since large number of sensor nodes is densely deployed, neighbour nodes may be very close to each other. Hence, multihop communication in sensor networks is expected to consume less power than the traditional single hop communication. Furthermore, the transmission power levels can be kept low, which is highly desired in covert operations. Multihop communication can also effectively overcome some of the signal propagation effects experienced in long-distance wireless communication.

In Hop-by-Hop message authentication scheme based on source anonymous message authentication (SAMA) concept was introduced. Its design inherits the advantage of avoiding the use of built-in threshold and also uses single equation based on Elliptic Curve Cryptography for verification. Major problem identified concerning the Hop-by-Hop message authentication scheme, was the lack of trustworthiness in the routing information. Thus reliability and scalability cannot be fully maintained. The novel approach used for alleviating this problem was to use a Trust based scheme which helps to maintain better results in terms of trustworthiness, packet delivery ratio and energy conservation. Most importantly this scheme doesn’t require the knowledge of any geographic information to provide an energy efficient routing.

The nature of WSNs complicates the security requirements and adds difficulties in solving security problems. One main reason is that the design of a routing protocol is biased towards solving the problem of power limitations and reducing communication overhead, while keeping security concerns in a later phase to be integrated with the current routing solutions. Thus, the major contributions of this work are as follows:

- To provide energy-efficient routing and reliable trust.

- To secure multi-hop routing in WSNs against intruders misdirecting the multi-hop routing by evaluating the trustworthiness of neighbouring nodes.

The rest of the paper is organized as follows. Section II gives an overview of the system using elaborates the architecture of existing system i.e., Hop-by-Hop concept. Section III includes problem formulation followed by section IV which provides details about the proposed work. Simulation and Analysis is explained in section V. Section VI concludes the whole work.

II. SYSTEM OVERVIEW

A. *Assumptions:*

The wireless sensor network consists of a large number of sensor nodes. Each node can be a data source or a data sink, and is capable of communicating with its neighboring nodes directly. The whole network is fully connected through multi-hop communications. It is assumed that there is a SS that is responsible for generating, storing and distributing the security parameters among the network. This server will never be compromised. However, after deployment, the sensor nodes may be captured and compromised by attackers. Once compromised, all information stored in the sensor nodes can be accessed by the attackers. The compromised nodes can be reprogrammed and fully controlled by the attackers. However, the compromised nodes will not be able to create new public keys that can be accepted by the SS and other nodes. This hop-by-hop node authentication was implemented without any threshold limitation, and has performance better than the symmetric-key based schemes. The distributed nature of the algorithm makes the scheme suitable for decentralized networks. Based on the above assumptions, this work considers both passive attacks and active attacks.

B. *Design Steps:*

The Hop-by-Hop SAMA concept includes the following steps:

1. Security Server (SS) model selection.
2. Registration of nodes to security server.
3. Anonymous message generation by nodes.
4. Verification of message authenticity.
5. Appropriate selection of Ambiguity Set (AS).
6. Selection of AS by the message source node from the public key list in the SS
7. Verification of Source privacy.

Below figure shows the schematic view of the Ambiguity set selection process.

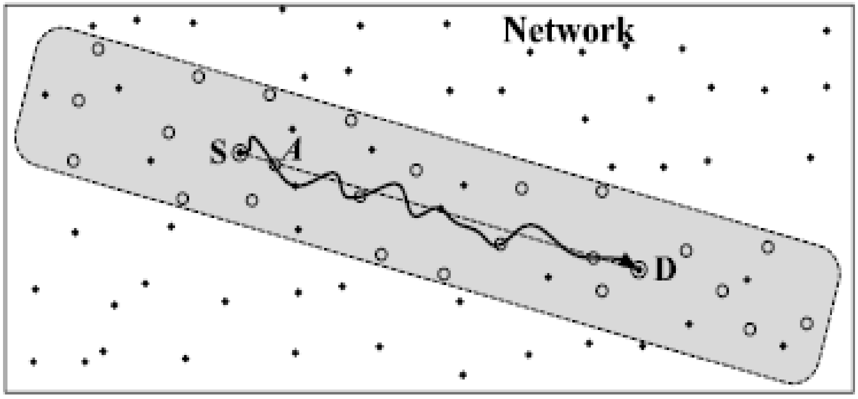

Fig.1. Illustration of AS selection in active routing

Fig.1 shows a network with large number of sensor nodes. Out of which a separate set of nodes are categorized to form the main set i.e, the Ambiguity Set or AS. The main specialty of this set is that the message source node is hidden inside this set such that, the chance of an attack from the intruders to track the sender node makes them difficult. Also, here the source-destination pair selection will be held within a predefined distance range from the routing path.

III. PROBLEM FORMULATION

Even though the routing protocols provide the encryption and authentication for routing information, still a malicious node participate in the network using another valid nodes identity to overcome this drawback various routing protocols such as gossiping-based routing protocols provide certain protection against attackers by selecting random neighbours to forward packets, but becomes an overhead in propagation time and energy use. Thus WSNs becomes more secure when they provide energy efficiency and cost worthiness. This can be incorporated in the existing work with least efforts producing a secure and efficient fully-functional protocol thus reducing the cost of an independent protocol.

Some of the challenges encountered in the SAMA concept includes:

- Continuous monitoring of traffic between previous hop transmissions.
- No trusted authority to trust the nodes in its routing decisions.
- Knowledge of geographic information such as time synchronization between the nodes.

Of the above mentioned challenges, reliable trust and energy efficient routing with clear data delivery are of utmost importance. In hop-by-hop message authentication scheme, the source node performs the function of key exchange, then the selection of SS and AS is performed to provide message authentication, followed by the verification of source privacy. And finally, the data transmission towards the destination.

Data packets that are delivered from source to destination may not be secure, since the above scheme lacks security. These issues can adversely affect in some major application areas of WSNs.

IV. PROPOSED WORK

Trust is a belief that ensures entity as secure and reliable. Thus trust model is used to differentiate trust worthy and untrustworthy nodes in a network. It encourages trustworthy nodes to communicate and discourages untrustworthy nodes to participate in the network. Also, it increases the network lifetime, throughput and resilience of the wireless sensor network. Routing decisions are taken based on the trust on other nodes which is formed according to the evidence collected from previous interactions. Misbehaved nodes are identified and avoided to forward packets by using the trust mechanism. In this way, misbehaviour can be mitigated. For example, a trust-based routing protocol can collect the evidence of nodes misbehaving, form trust values of the nodes and select safest routes based on the trust metrics.

A. Network Model:

Each node will select a next-hop node based on its neighbourhood table, and broadcast its energy cost within its neighbourhood. To maintain this table, Energy Watcher and Trust Manager are the two main components which are used on the node to keep track of all events such as to record the energy cost and the trust level values of its neighbours. Below figure shows the simplified architectural view using trust model. Here a packet is selected after testing the trust value of each node with the fixed threshold.

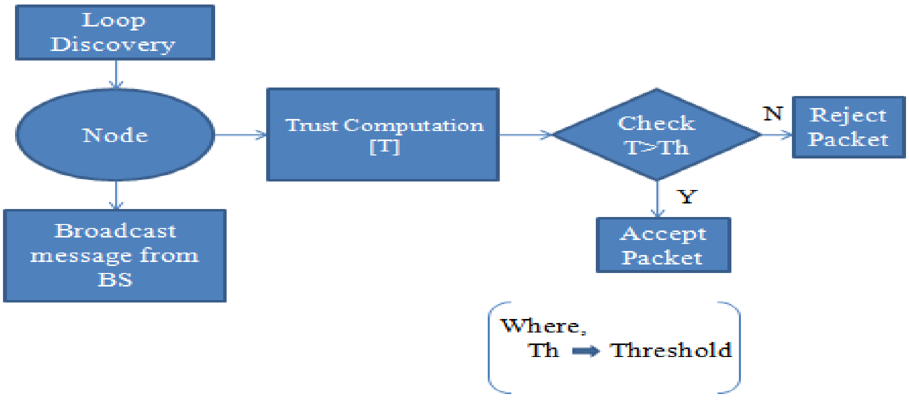

Fig.2. Overview of Trust Model

B. System Working:

While incorporating trust model into SAMA concept, first the stage of node deployment and hello packet transmission takes place in a network environment. Next a key Server is initialized which monitors the distance from each nodes and stores the respective values. Then the key sharing is initiated between nodes. And when the source node is identified, it dissipates RREQ packet to all nodes in the network and waits for the RREP. At this time all nodes calculate the trust values and store it in the neighborhood table. After a while the route reply is received and then the exact selection of the Ambiguity Set (AS) is made. Nodes satisfying the AS criteria will only be selected to perform active routing. And along with the trust values, energy cost is also estimated and stored in the neighborhood table. By considering the values in the table the source node selects its next hop neighbor and performs its data transmission towards the destination node.

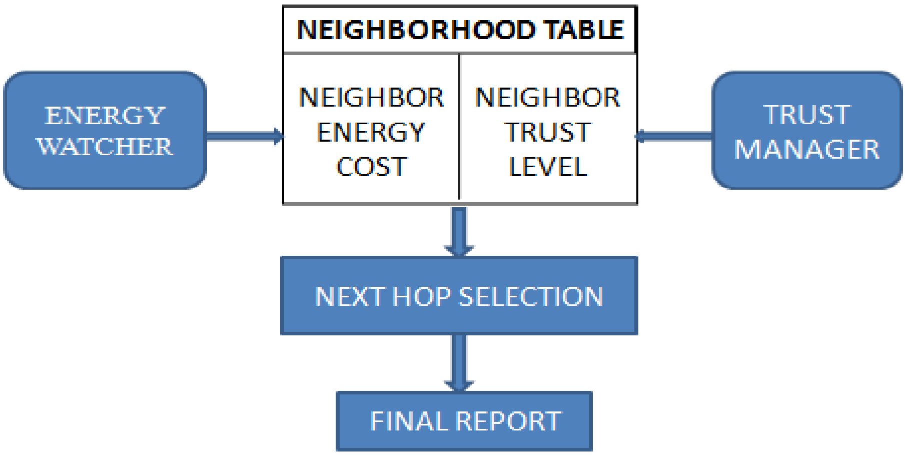

Fig.3. Structure of Neighbourhood Table

In this approach, Broadcast messages from the base station about data delivery and, Energy cost report messages from each node is collected to form the neighbourhood table. Some notations used in proposed work are shown in the table below.

Node	N
Trust Level	T
Energy Cost	EN
Average Energy Cost	EN→b

C. Trust Manager and Energy Watcher Details:

For each neighbour b of N, TNb denotes the trust level of b in N’s neighbourhood table. At the beginning stage, each neighbour is given a neutral trust value as 0.5. After the occurrence of any event, the relevant neighbour’s trust levels are updated. And this trust value is decided based on network loop discovery. Next the node send packet and keep the id of the packet in the table. When the node receives some packet for forwarding it checks whether the packet is present in the neighbourhood table. If the packet is present in the NHT, it discards that packet and degrades the trust value by 0.1 else the packet is forwarded. And in case of attackers in the network the Trust Manager will effectively identify the low trustworthiness. Once the low trust level of an attacker is identified, the route selection procedure, according to its preference of trustworthy nodes, enables a valid node to avoid choosing an adversary as its next-hop node.

Next while considering the case of Energy Watcher, if node N decides that say node B should be its next- hop node after comparing energy cost and trust level. Then, N‘s energy cost is EN = ENb. The Energy cost of node is analysed as per the equation,

$$ENb = EN{\rightarrow}b \;+ Eb \qquad (1)$$

And EN→b as the average energy cost of successfully delivering a data packet from N to its neighbour b with one hop. In this work Trust values of node and least distance path are the two main parameters considered for routing path selection.

V. PERFORMANCE EVALUATION

In this section, the performance of data delivery is estimated and a comparison is made between Hop-by-Hop message authentication with SAMA concept and that with Trust incorporated SAMA concept.

The simulations are done using NS-2 (Version 2.35). The total number nodes deployed are taken to be 50. Among these nodes, one node will act as a key server at the initial stage. The simulation area is taken to be 1600m×1000m. The nodes are configured with certain parameters like receive power, transmit power, idle power, sleep power etc. The routing protocol used here is Ad hoc on demand Multipath Distance Vector (AOMDV), which is a multi-path extension of AODV.

VI. SIMULATION RESULTS

In this section, the simulation results of various performance metric with respect to time for both hop-by-hop message authentication scheme and proposed system are plotted. The simulation plot of the proposed system is represented using green color and for hop-by-hop message authentication scheme, it is shown using red color. Comparison plots of throughput and packer delivery ratio are shown below. Fig.4 shows the plot of throughput which is high for the proposed work. Thus, it is clear that the rate of successful packet delivery at the destination is high using the trust model.

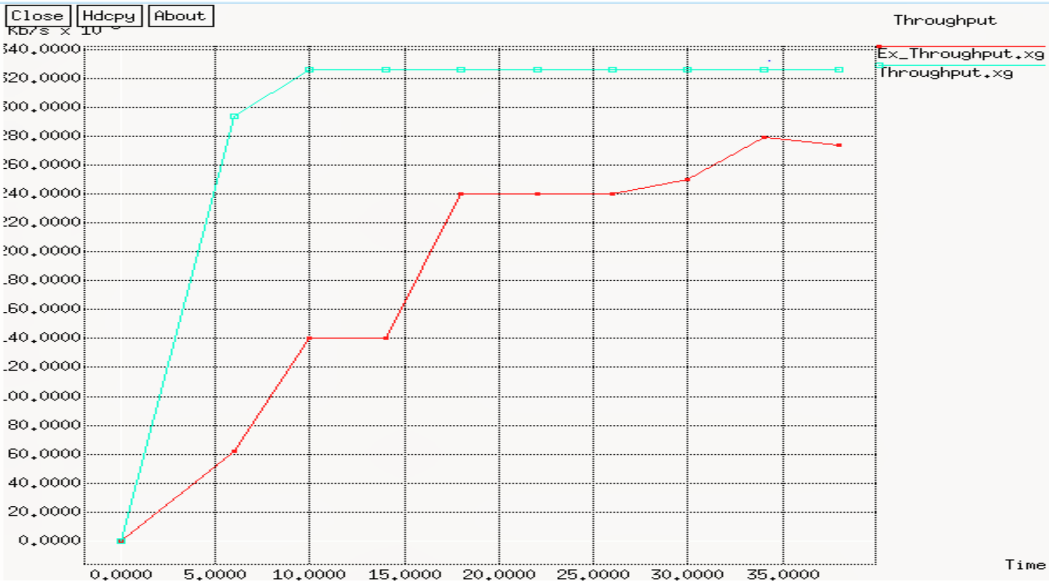

Fig.4. Comparison of Throughput

And Fig.5 shown below gives the plot of packet delivery ratio.

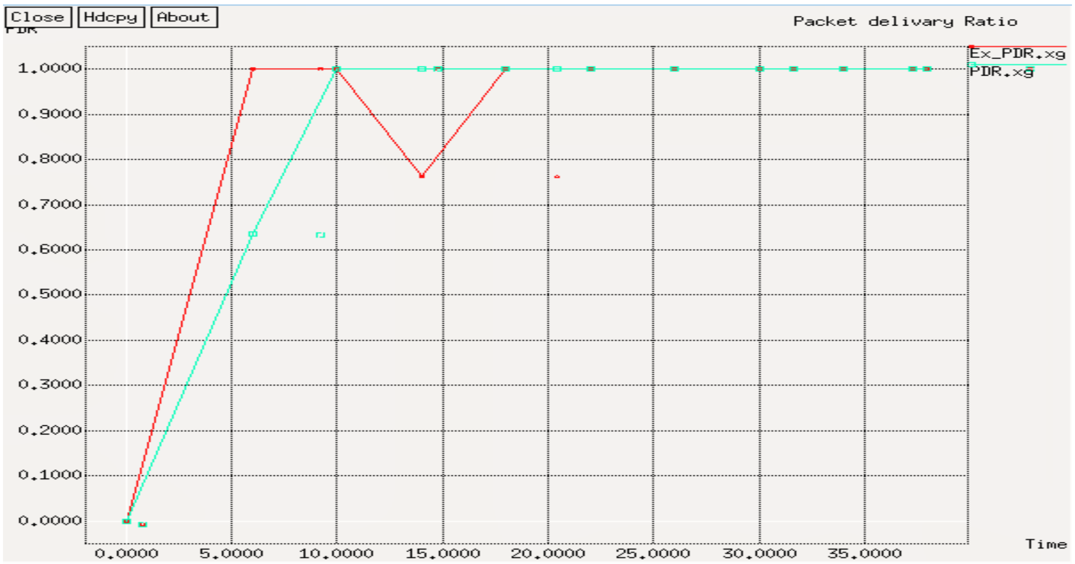

Fig.5. Comparison of Packet Delivery Ratio

And from this plot it is clear that, the proposed work has delivered maximum number of packets to the destination with negligible drop.

VII. CONCLUSION

Wireless sensor networks are models for applications to report detected events of interest, such as forest fire monitoring and military surveillance. These networks include battery powered senor nodes with exceptionally limited processing abilities. With a narrow radio communication range, a sensor node wirelessly passes messages to a base station via a multi-hop path. Though, the multi hop routing of WSNs often becomes the target of wicked attacks. Thus this work mainly contributes to secure the WSNs and to regularize the multi-hop routing techniques. A novel and efficient Hop-by-Hop authentication scheme based on SAMA was applied to a message to provide message content authenticity. This scheme can also provide message source privacy.

The major problem identified concerning the Hop-by-Hop message authentication scheme, was the lack of trustworthiness in the routing information's. Thus reliability and scalability cannot be fully maintained. The novel approach used for alleviating this major disadvantage includes a Trust model which helps to maintain better results in terms of trustworthiness, packet delivery ratio and energy conservation. Most importantly this scheme doesn't require the knowledge of any geographic information to provide an energy efficient routing. Here the simulation is carried out in NS-2 to find the performance of the network with and without the proposed scheme. And finally the simulation results shows the trust model increases the packet delivery ratio of the network against selective forwarding attack and thereby achieve High throughput, Energy Efficiency, scalability and adaptability.

REFERENCES

[1] Jian Li, Yun Li, Jian Ren, Senior Member, IEEE, and Jie Wu, Fellow, IEEE, "Hop-by-Hop Message Authentication and Source Privacy in Wireless Sensor Networks", IEEE Transactions On Parallel and distributed system, Vol. 25, No. 5, May 2014.

[2] M. Albrecht, C. Gentry, S. Halevi, and J. Katz, "Attacking Cryptographic Schemes Based on 'Perturbation Polynomials'," Report 2009/098, http://eprint.iacr.org/, 2009.

[3] 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 Intl Conf. Distributed Computing Systems (ICDCS), pp. 11-18, 2008.

[4] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci.A survey on sensor networks. IEEE Communications Magazine, 40(8):102–114, August 2002.

[5] Guoxing Zhan, Weisong Shi, Senior Member, IEEE, and Julia Deng, "Design and Implementation a Trust-Aware Routing Framework for WSNs," IEEE Transactions on dependable and secure computing, 2014.