Enhanced Pre Existing Routing Model for WSN Using Hop-by-Hop Message Authentication and Emap Protocol

Ms. M. Ramya [1]
PG Scholar,
Department of Computer Science and Engineering,
Vivekanandha College of Technology for Women,
Elayampalayam, Thiruchengode Tamilnadu,
India.

Mrs. D. Sathiya[2]
Assistant professor,
Department ofComputer Science and Engineering,
Vivekanandha College of Technology for Women,
Elayampalayam, Thiruchengode. Tamilnadu,
India.

***Abstract*—The proposed Solution of the Message authentication is one of the most important ways to stop unauthorized and corrupted messages from being forwarded to wireless sensor networks (WSNs). Message authentication schemes can largely be divided into two categories: public-key based approaches and symmetric-key based approaches. The symmetric-key based approach requires complex key management, lacks scalability, and is irrepressible to large numbers of node concession attacks since the message sender and the receiver have to share a secret key.The shared key is used by the sender to generate a message authentication code (MAC) for each transmitted message. However, for this method, the authenticity and integrity of the message can only be aerified by the node with the mutual secret key, that is generally shared by a group of sensor nodes.For this reason, many message authentication schemes have been developed, based on public-key cryptosystem. However, both symmetric and public-key methods have the limitations of high computational and communication overhead towords the addition to lack of scalability and flexibility to node compromise attacks.To address these issues, a scalable authentication scheme based on elliptic curve cryptography (ECC) and (GECC) has been proposed While enabling intermediate nodes authentication, the proposed scheme allows any node to transmit an unlimited number of the message, message source privacy, and multiple base station environments.**

***Keyword:*wireless sensor network, message authentication code, message source, privacy, base station.**

I INTRODUCTION

Message authentication plays an important key role in the waiting unauthorized and depraved messages from being forwarded in networks to save the preceding sensor energy. The symmetric-key based approach requires complex key management, lacks scalability, and is not resilient to large numbers of node compromise attacks since the message sender and the receiver have to share a secret key. The shared key is send by the user to generate a message authentication code (MAC) for each transmitted message. However, for this method, the authenticity and integrity of the message can only be verified by the node with the shared secret key, which is generallyshared by a group of sensor nodes. An intruder can compromise the key by capturing a single sensor node. In addition, this method adds to work in multicast networks.

II RELATED WORKS

A. Abhay Kumar Rai

In the MANET-Internet communication are integrated, a connection could be disrupted either by attacks Internet connectivity or routing protocols. Due to this reason, almost all possible attacks on the traditional ad hoc networks also exist in the integrated wired and mobile ad-hoc network.Security is an important issue in the integrated MANET-Internet environment because in this environment we have to consider the attacks on Internet connectivity and also on the ad hoc routing protocols. The focus of this work is on different types of attacks on integrated MANET-Internet communication.

1) Bogus Registration

A bogus registration active attack in which an attacker does a registration with a bogus care-of address by masquerading itself as someone else. By advertising fraudulent beacons, an attacker might be able to attract an MN (mobile node) to register with the attacker as if MN has reached HA (home agent) or FA (foreign agent).

2) Forged FA

It is a form of network attack in which a node advertises itself as a fraudulent FA then MN's under the coverage of the forged FA may register with it. Now, forged FA can capture the sensor network data and may disrupt the proper functioning of the network.

3) Snooping

Snooping is an unauthorized access to another person's data .Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing.

B ..Darren Hurley-Smith

The increasing autonomy of Mobile Ad Hoc Networks (MANETs) has enabled large-scale unguided missions, such as agricultural planning, conservation, and similar surveying tasks. have expressed great interest in such ventures; raising the question of security as the application of such systems in potentially hostile environments becomes the of such networks. Preventing theft, destruction of such MANETs through cyber-attacks has become a focus for many researchers as a result. To support routing, broadcast updates and efficient MANET communication, a Virtual Closed Network (VCN) architecture is proposed. By supporting private, in unicast, multicast and broadcast modes, VCNs provide the alternative to VPNs when securing MANETs. A VCN will extend protection beyond confidentiality, integrity, and authentication, by providing services that ensure routes. This provides weak guarantees of delivery, weak due to the fact that medium-control is not a part of most VCNs, and so disruption of the may still cause loss of data.

C . *JAKOB POJDA*

Unmanned Aerial Vehicles (UAVs) are an emerging technology offering new opportunities for innovative applications and efficient overall process management in the areas of public security, cellular networks, and surveying. A key factor for the optimizations yielded by this technology is an advanced mesh network design for fast and reliable information sharing between UAVs. The protocols are analyzed by means of good put in one static and one mobile scenario using the same embedded hardware platform installed at UAVs in current research projects. Hence, given the aforementioned routing protocols, we recommend to currently use open80211s or batman advanced to establish a reliable multi-hop mesh network for swarming applications. OLSR uses the MultiPoint Relaying (MPR) method, which is the key concept of this protocol. Herewith, nodes select only a subset of neighboring nodes to relay data instead of every node acting as a relay. These nodes are called MPR. Any node, which is not in the MPR set, can read and process each packet but does not retransmit it. This optimization works well for large and dense networks. The larger and denser the network, the better is the optimization achieved. This paper analyses the performance of four mesh routing protocols on layer-2 and 3, to relay traffic between UAVs in regions with insufficient network coverage.

D . Rutvij Jhaveri

MANETs have a individual characteristics like dynamic topology, wireless radio medium, limited resources and lack of consolidate administration; as a result, they are vulnerable to different types of attacks in different layers of the protocol stack. Each node in a MANET is capable of acting as a router. Routing is one of the aspects having various security concerns. In this paper, we will present the survey of common Denial-of-Service (DoS) attacks on network layer namely Wormhole attack, Blackhole attack and Grayhole attack which are serious threats to MANETs.

III METHODOLOGY

The WSNs are assumed to consist of a large number of sensor nodes. We assume that each sensor node knows its relative location in the sensor domain and is capable of communicating with its neighboring nodes directly using geographic routing. The whole network is fully connected through multi-hop communications. Security server (SS) is responsible for generation, storage, and distribution of the security parameters of the network. The compromised nodes can be fully controlled and reprogrammed 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.

In this project considers two types of attacks launched by the adversaries: passive and active attack. Passive attacks, the adversaries could eavesdrop on messages transmitted in the network and perform traffic analysis. Active attacks can only be launched from the compromised sensor nodes. Once the sensor nodes are arranged and adversaries with the obtained of all the information stored in the compromised nodes, and the including the security parameters of the compromised nodes. The adversaries can modify the contents of the messages, and inject their own messages. In addition, the scheme can also provide message source privacy. Also, multiple base station environments are considered.

Message authentication plays an important key role in the waiting unauthorized and corrupted messages from being forwarded in networks to save the precious sensor energy. The symmetric-key based approach requires complex key management, lacks scalability, and is not resilient to large numbers of node compromise attacks since the message sender and the receiver have to share a secret key. However, for this method, the authenticity and integrity of the message can only be verified by the node with the shared secret key, which is generally shared by a group of sensor nodes. An intruder can compromise the key by capturing a single sensor node. In addition, this method adds to work in multicast networks

A. NETWORK CONSTRUCTION

In this module, ‘n’ number of nodes is created with hop distance from base station node. The details are saved in ‘WSN’ table.

B. DISPLAY NETWORK

In this module, Wireless Sensor Network is displayed graphically like the one in the following figure.

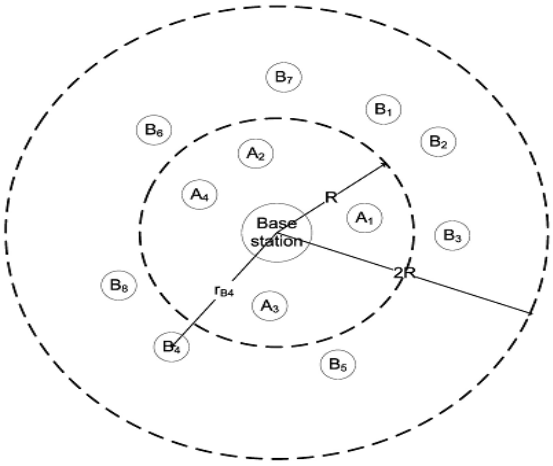

Fig. 3.1 DISPLAY NETWORK

C. MESSAGE GENERATION IN SOURCE NODE

In this module, the message is generated in the source node. The message receiver should be able to verify whether a received message is sent by the node that is claimed, or by a node in a particular group.

1)Identity and location privacy: The adversaries cannot determine the message sender's ID and location by analyzing the message contents or the local traffic.

The message is generated like the following:

Generate (m, Q1, Q2,...,Qn). Given a message m and the public keys Q1, Q2,...,Qn of the AS (Ambiguous Set) S={A1, A2, ... , An}, the actual message sender At, 1 <= t <= n, produces an anonymous message S(m) using its own private key it.

Verify S(m). Given a message m and an anonymous message S(m), which includes the public keys of all members in the AS, a verifier can determine whether S(m) is generated by a member in the AS.

The security requirements include:

2)Sender ambiguity. The probability that a verifier successfully determines the real sender of the anonymous message is exactly 1=n, where n is the total number of members in the AS.

3)Unforgeability. An anonymous message scheme is unforgeable if no adversary, given the public keys of all members of the AS and the anonymous messages $m_1, m_2,...,m_n$ adaptively chosen by the adversary, can produce the message.

The main idea is that for each message m to be released, the message sender, or the sending node, generates a source anonymous message authenticator for the message m. The generation is based on elliptic curves. For a ring signature, each ring member is required to compute a forgery signature for all other members in the AS.

The AS includes n members, A1, A2, ... ,An, for example, S={A1,A2, ... ,An}, where the actual message sender Alice is At, for some value t; 1 <= t <= n. In this project, we will not distinguish between the node Ai and its public key Qi. Therefore, we also have S={Q1, Q2, ..., Qn}.

4)Authentication generation algorithm: Suppose m is a message to be transmitted along with base station node id. The private key of the message sender Alice is at; 1 <= t <= n. To generate an efficient scheme for message m, Alice performs the following three steps:

1. Select a random and pairwise different ki for each 1 £ I £ n – 1, I ¹ t and compute RI from (RI, Yi) = k_id.
2. Choose a random ki□□Zp and compute r_t from (rt, yet)= k_t - åi¹ t $r_i h_i Q_i$ such that r_t□ 0 and r_t ¹
3. $_i$RI for any I <> t, where h_i = h(m, $_i$RI).
4. Compute s = k_t + □$_i$□$_t$□k_i + $r_t d_t h_t$ mod N.

The scheme of the message m is defined as:

S(m) = (m, S, r1, y1, ... , r_n, $_{in}$, s).

D. MESSAGE VERIFICATION IN SINK NODE OR BASE STATION

1)Verification algorithm: For Bob to verify the scheme (m, S, r1, y1,..., r_n, $_{in}$, s), he must have a copy of the public keys Q1, ... , Qn. Then he:

1. Checks that Q_i□□ O, i = 1, ….,n otherwise invalid.
2. Checks that Q_i, i = 1, …., n lies on the curve.
3. Checks that nQ_i = O, i = 1, …., n.

After that, Bob follows these steps:

1. Verify that ri, Yi, i = 1,….n and s are integers in [1, N -1]. If not, the signature is invalid.
2. Calculate h_i = h(m, r), where his the same function used in the signature generation.n
3. Calculate (x0, y0) = sG - □□rih_iQ_i i=1
4. The signature is valid if the first coordinate of □$_i$(RI, Yi) equals $x_{0.}$ invalid otherwise.

In fact, if the scheme has been correctly generated without being modified, then we compute:

$$
\begin{aligned}
(x_0, y_0) &= sG - \sum_{i=1}^{n} r_i h_i Q_i \\
&= \left(k_t + \sum_{i \neq t} k_i + r_t d_t h_t\right) G - \sum_i r_i h_i Q_i \\
&= \sum_{i \neq t} k_i G + \left(k_t G - \sum_{i \neq t} r_i h_i Q_i\right) \\
&= \sum_{i \neq t} (r_i, y_i) + (r_t, y_t) \\
&= \sum_i (r_i, y_i).
\end{aligned}
$$

IV SYSTEM ARCHITECTURE

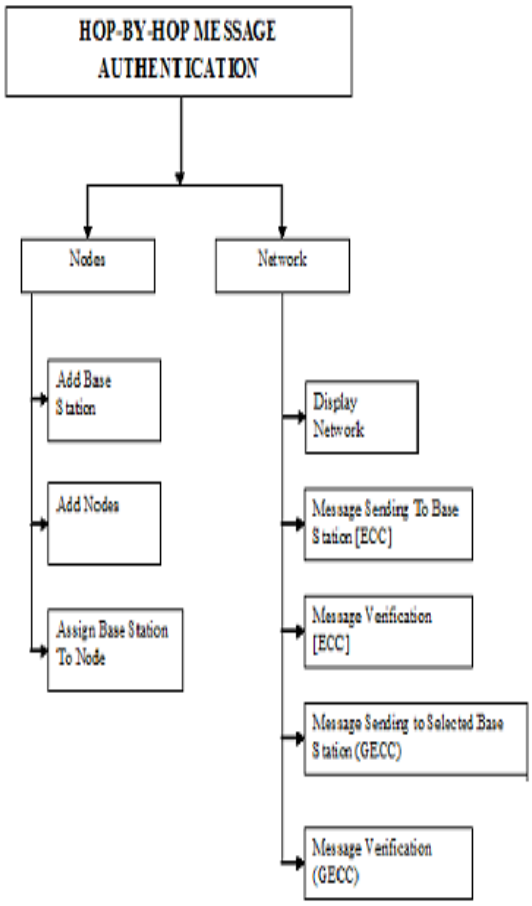

Fig: 4.1 SYSTEM ARCHITECTURE

V CONCLUSION

This proposed project is to use message sending, a physical property associated with each wireless device that is hard to falsify and irrepressible on cryptography as the basis for detecting numerous attackers in wireless networks. It provided a theoretical analysis of using the hop by hop based inherited from wireless nodes for attack detection.

The approach can be detects both the presence of attacks as well as determine the number of adversaries we can localize any number of attackers and eliminate them. In addition, a Multi hop-based node message sending and compromise detection scheme is proposed using the Geometrical elliptic curve cryptography (GECC). Furthermore, several possible attacks are described against the proposed scheme and proposed multi-hop based measures against these attacks. The scheme is evaluated in simulation under various scenarios. The experimental results show that the scheme quickly detects untrustworthy multihop with a small number of trust reports.

VI FUTURE ENHANCEMENTS

In future, the scheme may evaluate against various types of attacker models. It is believed that a game theoretic model is suited for this evaluation. A variety of strategies may be studied that may be taken by detector and adversary.

VII. REFERENCES

[1] Bhattacharya .S and T. Basar, 2010 Game-theoretic analysis of an aerial jamming attack on a UAV communication network,in American Control Conference (ACC),. IEEE, 2010, pp. 818–823.

[2] Jhaveri R.H, S. J. Patel, and D. C. Jinwala,2012 Dos attacks in mobile ad hoc networks: A survey in Advanced Computing & Communication Technologies (ACCT), Second International Conference on. IEEE, 2012, pp. 535–541.

[3] Rai A.K, R. R. Tewari, and S. K. Upadhyay, 2010 Different types of attacks on integratmanet-internet communication, International Journal of Computer Science an Security, vol. 4, no. 3, pp. 265–274.

[4] PankajJalole, An Integral approach to software engineering, ,Narosa publishing Home-3rd Edition.

[5] Ye.F, H. Lou, S. Lu, and L. Zhang, 2004 Statistical En-Route Filtering of Injected False Data in Sensor Networks, Proc. IEEE INFOCOM.

[6] Hurley-Smith.D, J. Wetherall, and A. Adekunle,2015 Virtual closed networks: A secure approach to autonomous mobile ad hoc networks," in 10th International Conference for Internet Technology and Secured Transactions (ICITST). IEEE, pp. 391–398.

[7] PojdaJ,A.Wolff, M. Sbeiti, and C. Wietfeld2011performance analysis of mesh routing protocols for UAV swarming applications,in wireless Communication Systema (ISWCS),8th International Symposium on.IEEE,2011,pp 317-3.