ECC: Elliptic Curve Cryptography-based Watchdog for Detecting Malicious Nodes

M. Rudhra*, N. Sathya Lakshmi**, S. Thenmozhi***, A. Tamizhenthi**** & Dr. N. Nandhagopal*****

*UG Student, S.K.P Engineering College, Thiruvannamalai, Tamil Nadu, INDIA.
**UG Student, S.K.P Engineering College, Thiruvannamalai, Tamil Nadu, INDIA.
***UG Student, S.K.P Engineering College, Thiruvannamalai, Tamil Nadu, INDIA.
****UG Student, S.K.P Engineering College, Thiruvannamalai, Tamil Nadu, INDIA.
*****Professor, S.K.P Engineering College, Thiruvannamalai, Tamil Nadu, INDIA.

***Abstract*—**Mobile Ad-Hoc Networks (MANETs) assume that mobile nodes voluntary cooperate in order to work properly. This cooperation is a cost-intensive activity and some nodes can refuse to cooperate, leading to a node behaviour. Thus, the overall network performance could be seriously affected. Many message authentication schemes have been developed, based on either symmetric-key cryptosystems or public-key cryptosystems. Most of them, however, have the limitations of high computational and communication overhead in addition to lack of scalability and resilience to node compromise attacks. To address these issues, a polynomial-based scheme was recently introduced. However, this scheme and its extensions all have the weakness of a built-in threshold determined by the degree of the polynomial. In this paper, we propose a scalable authentication scheme based on Elliptic Curve Cryptography (ECC). While enabling intermediate nodes authentication, our proposed scheme allows any node to transmit an unlimited number of messages without suffering the threshold problem. In addition, our scheme can also provide message source privacy.

***Keywords*—**Elliptic Curve Cryptography; Malicious Nodes; MANET; Node Behaviour; Watchdog.

***Abbreviations*—**Elliptic Curve Cryptography (ECC); Mobile ad-Hoc Networks (MANETs).

I. INTRODUCTION

AN mobile ad-hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any stand-alone infrastructure or centralized administration. Mobile Ad-hoc networks are self-organizing and self re-configuring multihop wireless networks where, the structure of the network changes dynamically. This is mainly due to the mobility of the nodes. Nodes in these networks utilize the same random access wireless channel, cooperating in a friendly manner to engaging themselves in multihop forwarding. The nodes in the network not only act as hosts but also as routers that route data to/from other nodes in network. In mobile ad-hoc networks where there is no infrastructure support as is the case with wireless networks, and since a destination node might be out of range of a source node transmitting packets routing procedure is always needed to find a path so as to forward the packets appropriately between the source and the destination. Within a cell, a base station can reach all mobile nodes without routing via broadcast in common wireless networks. In the case of ad-hoc networks, each node must be able to forward data for other nodes. This creates additional problems along with the problems of dynamic topology which is unpredictable connectivity changes [Li et al., 1].

MANETS rely on wireless transmission, a secured way of message transmission is important to protect the privacy of the data. An insecure ad-hoc network at the edge of an existing communication infrastructure may potentially cause the entire network to become vulnerable to security breaches. In mobile ad hoc networks, there is no central administration to take care of detection and prevention of anomalies. Mobile devices identities or their intentions cannot be predetermined or verified. Therefore nodes have to cooperate for the integrity of the operation of the network. However, nodes may refuse to cooperate by not forwarding packets for others for selfish reasons and not want to exhaust their resources. Various other factors make the task of secure communication in ad hoc wireless networks difficult include the mobility of the nodes, a promiscuous mode of operation, limited processing power, and limited availability of resources such as battery power, bandwidth and memory. Therefore nodes have to cooperate for the integrity of the operation of the network. Nodes may refuse to cooperate by not forwarding packets for others for selfish reasons and not want to exhaust their resources. In ad hoc networks devices (also called nodes) act both as computers and routers. Most routing protocols nodes to exchange network topology information in order to establish communication routes. This information is sensitive and may become a target for malicious adversaries who intend to attack the network or the applications running on it.

There are two sources of threats to routing protocols. The first comes from external attackers. By injecting erroneous

routing information, replaying old routing information or distorting routing information, an attacker could successfully partition a network or introduce a traffic overload by causing retransmission and inefficient routing. The second and more severe kind of threat comes from compromised nodes, which might (i) misuse routing information to other nodes or (ii) act on applicative data in order to induce service failures. The provision of systematic approaches to evaluate the impact of such threats on particular routing protocols remains an open challenge today. Attacks on ad hoc are classified into non disruptive passive attacks and disruptive active attacks. The active attacks are further classified into internal attacks and external attacks are carried out by nodes that do not belong to network and can be prevented by firewalls and encryption techniques. Internal attacks are from internal nodes which are actually authorized nodes and part of the network hence it is difficult to identify [Shailender Gupta & Singla, 2].

II. PROPOSED SYSTEM

We introduces Elliptic Curve Cryptography (ECC) scheme for detecting selfish nodes that combines local watchdog detections and the dissemination of this information on the network. This scheme is secure against adaptive chosen-message attacks. This scheme enables the intermediate nodes to authenticate the message so that all corrupted message can be detected and dropped to conserve the sensor power. While achieving compromise resiliency, flexible-time authentication and source identity protection, our scheme does not have the threshold problem. It develop a source anonymous message authentication code on elliptic curves that can provide unconditional source anonymity. It offer an efficient hop-by-hop message authentication mechanism for WSNs without the threshold limitations. It devices network implementation criteria on source node privacy protection in WSNs. It propose an efficient key management framework to ensure isolation of the compromised nodes. The distributed nature of our algorithm makes the scheme suitable for decentralized networks [Hernandez-Orallo et al., 3].

III. ARCHITECTURE DESIGN

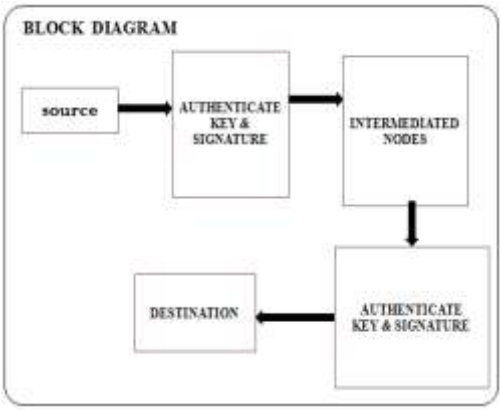

Figure 1: Block Diagram

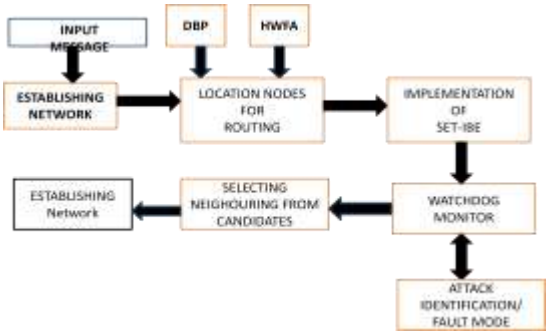

Figure 2: Working

IV. TECHNIQUES

A number of secure routing schemes have been brought forward for intrusion-detection in MANETs.

4.1. WATCHDOG

It is responsible for detecting malicious node misbehaviours in the network. Watchdog detect malicious misbehaviour by promiscuously listening to its next hop's transmission. It will improve the throughput of network with the presence of malicious nodes [Lauter, 4].

4.2. TWOACK

In order to overcome the drawbacks in watchdog, a new scheme is proposed that is TWOACK, to resolve the receiver collision and limited transmission power problems of Watchdog, TWOACK detect misbehaviour links by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination.

4.3. AACK

It is similar to TWOACK, AACK is an acknowledgment-based network layer scheme which can be considered as a combination of a scheme called TACK (identical to TWOACK) and an end-to-end acknowledgment scheme called ACKnowledge (ACK). It can significantly reduce overhead when compared with TWOACK. It schemes are largely depend on the acknowledgment packets. Hence, it is crucial to guarantee that the acknowledgment packets are valid and authentic but they suffer from the problem that they fail to detect malicious nodes with the presence of false misbehaviour report and forged acknowledgment packets.

Another drawback of most previous schemes is the significant amount of unwanted network overhead. Due to the limited battery power nature of MANETs, such overhead can easily degrade the life span of the entire network.

V. PROJECT DESCRIPTION

5.1. Routing Attacks in MANET

The malicious node (s) can attacks in MANET using different ways such as sending fake messages several times, fake routing information and advertising fake links to disrupt

routing operations. In the following subsection, current routing attacks and its countermeasures against MANET protocols are discussed in detail [Liu & Ning, 5].

5.2. Security Attacks on MANET

Malicious and selfish nodes are the ones that fabricate attacks against physical, data link, network, and application layer functionality. Current routing protocols are exposed to two types of attacks [Du et al., 6].

5.2.1. Active Attacks

In active attack, information is inserted to the network and thus the network operation or some nodes may be harmed. Through which the misbehaving node has to bear some energy costs in order to perform some harmful operation, and Nodes that perform active attacks with the aim of damaging other nodes by causing network outage are considered to be malicious.

5.2.2. Passive Attacks

In a passive attack, malicious node either ignores operations supposed to be accomplished by it. That mainly consists of lack of cooperation with the purpose of energy saving Nodes that perform passive attacks with the aim of saving battery life for their own communications are considered to be selfish. Selfish nodes can severely degrade network performances and eventually partition the network.

5.2.3. Tunnelling /Wormhole(Network Layer Attack)

Tunnelling attack is also called wormhole attack. In a tunnelling attack, an attacker receives packets at one point network, "tunnels" them to another point in the network, and then replays them into the network from that point it is called tunnelling attack because the colluding malicious nodes are linked through a private network connection which is invisible at higher layers.

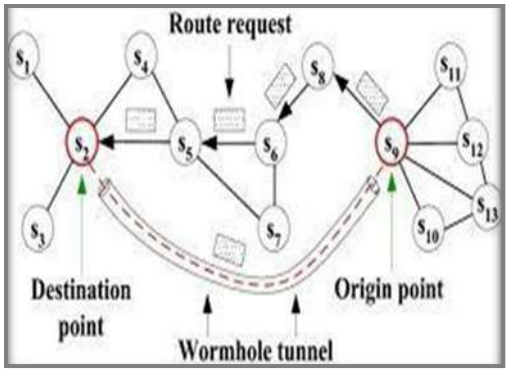

Figure 3: Network Layer Attack

5.2.4. Wormhole Attack Sybil Attack

Malicious nodes in a network may not only impersonate one node, they could assume the identity of several nodes, by doing so undermining(destroy) the redundancy(repeating) of many routing protocols. This attack is called the Sybil attack. Sybil attack tries to degrade the integrity of data, security and resource utilization that the distributed algorithm attempts to achieve. Sybil attack can be performed for storage, routing mechanism, air resource allocation and misbehaviour detection. Basically, any peer-to-peer network (especially wireless adhoc networks) is vulnerable to Sybil attack [Sundarajan & Shammugam, 7].

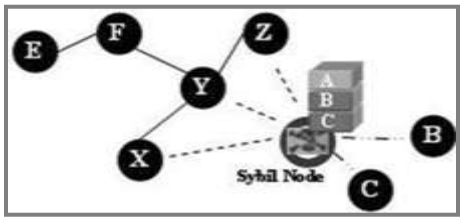

Figure 4: Sybil Attack

VI. FLOWCHART FOR WSN USING IN MILITARY APPLICATIONS

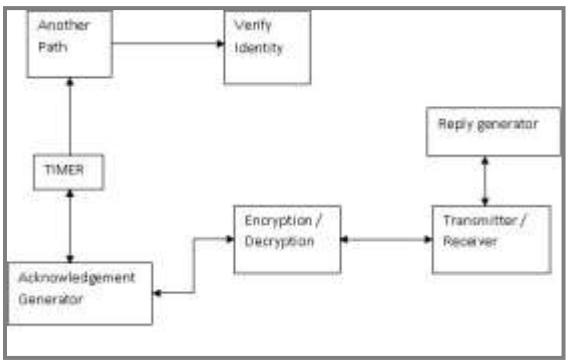

Figure 5: Flowchart

6.1. Secure Data Transmission

Networks of thousands tiny sensor devices, which have low processing power, limited memory and energy, play roles for an economical solution to some challenging problems, such as, traffic monitoring, building safety, border security, habitat monitoring, tsunami alarm, medical emergency response and so on. Undoubtedly security is an integral part of these applications. Authenticity of message is more important than confidentiality of data in this case. Consequently, if application does not consider adequate security measure then the intruder could find possible backdoor to feed highly abnormal information into the sensing devices and gain advantage of its own choice. If the data in adhoc are made available directly to the external party, then authentication and authorization of the external party must be ensured before allowing him/her to access data. Secure data communication are done using the following techniques in this paper.

6.2. Secured Route Discovery by SMT

Secured routes are provided by establishing an End-to-End security association between the source and the destination. This scheme won't consider the intermediate nodes that may exhibit arbitrary and malicious behavior. The source node S and destination node T negotiate a shared secret key- KS, T with the knowledge of each other's public key.

VII. MODULES

- Basic routing module
- Include hacking in basic routing module
- Secure Acknowledgement MRA

7.1. Basic Routing Module

- If the source has no route to the destination, then source v initiates the route discovery in an on-demand fashion
- After generating RREQ, node looks up its own neighbor table to find if it has any closer neighbor node toward the destination node.
- If a closer neighbor node is available, the RREQ packet is forwarded to that node.
- If no closer neighbor node is the RREQ packet is flooded to all neighbor nodes.

7.1.1. Include Hacking in Basic Routing Module

In this module attack issues will arise in to the network. Providing security to the attacks will be considered.

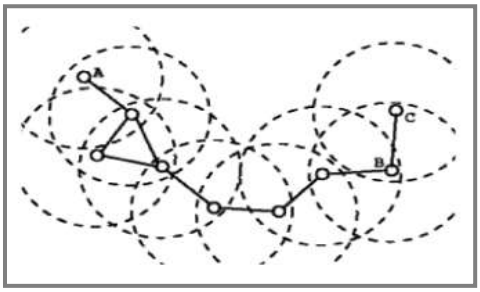

Figure 6: Basic Routing Module

7.2. Black Hole Attack

MANETs face different securities threats i.e. attack that are carried out against them to disrupt the normal performance of the networks. In these attacks, black hole attack is that kind of attack which occurs in Mobile Ad-Hoc networks (MANET). In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it.

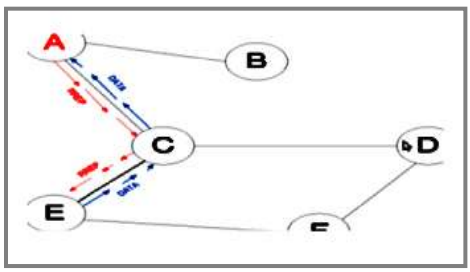

Figure 7: Black Hole Attack

7.2.1. Secure Acknowledgement

- In this module, we are implementing secure acknowledgement to detect misbehaving nodes in the routing environment.
- In this module we are ensuring that acknowledgement is authentic and untainted by Digital Signature.

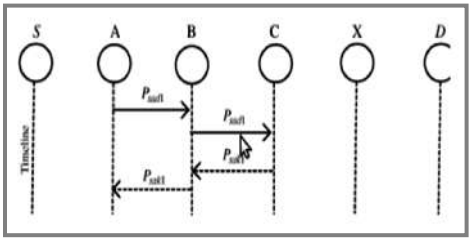

Figure 8: Secure Acknowledgement

In the above figure, S is the source node whenever it doesn't receives the acknowledgement it will start secure acknowledgement process within three-three nodes. Here A, B, C is the 1st group which node a sending one packet to node B, it will forward to node C after that both nodes B and C have to send acknowledgement to node A within time. If acknowledgement not received means it will report those nodes as misbehaving nodes to source node. But in this process there is a chance of false reports to avoid this we are implementing MRA.

7.2.2. MRA

- In this module we are avoiding false reports generated by the Misbehaving nodes.
- The main aim of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route.

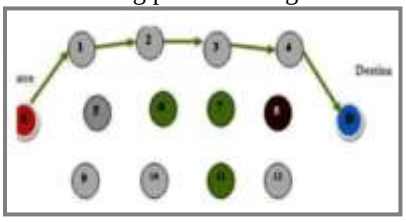

Figure 9: MRA

In the above figure we can observe that between source and destination there are multiple paths available in MANET. So, to avoid false reports in secure ACK scheme we will find another path between source and destination and source will check the reports which it gotten from intermediate nodes if any false report found means it will treat the node which sends that report as a misbehaving node.

VIII. SYSTEM IMPLEMENTATION

System implementation is a stage in a stage in the project where the where the theoretical designs turned into working system. The most crucial stage is the user confidence that the new system will work effectively and efficiently. performance of reliability of the system was tested and it

gained acceptance. The system was implemented successfully. Implementation is a process that means converting a new system into operation. Proper implementation is essential to provide a reliable system to meet organization requirements. During the implementation stage a live demon was undertaken and made in front of end-users. Implementation is a stage of project when the system design is turned into a working system. The stage consists of the following steps.

- Testing the developed program with sample data.
- Detection and correction of internal error.
- Testing the system to meet the user requirement.
- Feeding the real time data and retesting.
- Making necessary change as described by the user.

IX. OUTPUT DESIGN

Intelligent output design will improve systems relationships with the user and help in decision making. Outputs are also used to provide a permanent hardcopy of the results for latter consultations. The most important reason, which tempts the user to go for a new system is the output. The output generated by the system is often regarded as the criterion for evaluating the usefulness for the system. Here the output requirements use to be predetermined before going to the actual system design.

The output design is based on the following:

- Determining the various outputs to be presented to the user.
- Differentiating between inputs to be displayed and those to be printed.
- The format for the presentation of the outputs.

X. CONCLUSION

In this paper, we design an authenticated and anonymous routing protocol for MANETs in adversarial environments. The route request packets are authenticated by group signatures which can defend the potential active anonymous attacks without unveiling the node identities. The key-encrypted onion routing with a route secret verification message is designed to not only record the anonymous routes but also prevent the intermediate nodes from inferring the real destination. Compared to ANODR, AASR provides higher throughput and lower packets loss ratio in different mobile scenarios in the presence of adversary attacks. It also provides better support for the secure communications that are sensitive to packet loss ratio.

REFERENCES

[1] Y. Li, G.Su, D. Wu, D. Jin, L. Su & L. Zeng (2011), "The Impact of Node Selfishness on Multicasting in Delay Tolerant Networks", *IEEE Transactions on Vehicular Technology*, Vol. 60, No. 5, Pp. 2224–2238.

[2] C.K.N. Shailender Gupta & C. Singla (2011), "Impact of Selfish Node Concentration in MANETs", *International Journal of Wireless & Mobile Networks*, Vol. 3, No. 2, Pp. 29–37.

[3] E. Hernandez-Orallo, M.D. Serrat, J.C. Cano, C.M.T. Calafate & P. Manzoni (2012), "Improving Selfish Node Detection in MANETs using a Collaborative Watchdog", *IEEE Communication*, Vol. 16, No. 5, Pp. 642–645.

[4] K. Lauter (2004), "The Advantages of Elliptic Curve Cryptography for Wireless Security", *IEEE Wireless Communications*, Vol. 11, No. 1, Pp. 62-67.

[5] A. Liu & P. Ning (2008), "TinyECC: A Configurable Library for Elliptic Conference on Information Processing in Sensor Networks", *International Conference on Information Processing in Sensor Networks*, Pp. 245–256.

[6] W. Du, R. Wang & P. Ning (2013), "An Efficient Scheme for Authenticating Public Keys in Sensor Networks", *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, Pp. 58–67.

[7] T. Sundarajan & A. Shammugam (2014), "Modeling the Behavior of Selfish Forwarding Nodes to Stimulate Cooperation in Manet", *International Journal of Network Security and its Applications (IJNSA)*, Vol. 2.