Qos Based Secure Data Transmission Using Routing Driven Protocol In Mobile Adhoc Networks

N.Nathiya[1] P.Nandini[2]

**[1,2] Assistant Professor, Computer Science and Engineering
V.S.B.Engineering College, Karur,
Tamil nadu. India.**

Abstract

Operating in open and shared media, wireless communication is inherently less secure than wired communication. Even worse, mobile wireless devices usually have limited resources, such as bandwidth, storage space, processing capability, and energy, which make security enforcement hard. Compared with infrastructure-based wireless networks, security management for wireless ad hoc networks is more challenging due to unreliable communication, intermittent connection, node mobility, and dynamic topology. A complete security solution should include three components of prevention, detection, and reaction, and provides security properties of authentication, confidentiality, non-repudiation, integrity, and availability. The routing control messages are secured by using both public and shared keys, which can be generated on-demand and maintained dynamically. The message exchange mechanism also provides a way to detect attacks routing protocols, particularly the most difficult internal attacks. The routing metrics are obtained by combining the requirements on the trustworthiness of the nodes in the network and the Qos of the links. The simulation results have demonstrated the effectiveness of the proposed secure QoS routing protocol in both security and performance. It should be adaptive in order to trade-off service performance and security performance under resource limitation. Malicious node identification forms the main component of this project. Efficient, Energy-aware link-link authentication has been devised.

Keywords – Mobile adhoc networks, QOS, AODV, DSR.

I. INTRODUCTION

Wireless ad hoc networks start to be widely deployed in various environments. A particular challenging problem in designing such networks is how to detect the major attacks against the routing protocols while also provide some QoS support to the network traffic[1]. First, the routing protocols must be secured to defend attacks that may come from external or internal nodes. In an external attack, a malicious node masquerades as a trusted node although it does not participate in the routing process. It can generate floods of spurious service requests, such as DoS attack. In an internal attack, a malicious node may be a compromised or misconfigured node participating routing, or even colludes with other malicious nodes, which is called a Byzantine attack. It may advertise false routing information, not forward packet correctly, misroute, fabricate, modify, or simply drop packets [2]. Therefore, it is more difficult to detect the internal attacks. Second, the protocols must be integrated with QoS routing schemes to support the QoS [4] requirements of the carried traffic, for example, to minimize a cost under delay constraint, or minmax a cost caused by a single link failure or by co- channel interferences. The existing SRPs for ad hoc networks often avoid either the most challenging internal attacks, such as Byzantine behaviors, or the QoS requirements of the traffic.The fact that security is a critical problem when implementing MANETs is widely acknowledged. One of the different kinds of misbehavior a node may exhibit is selfishness [3]. A selfish node wants to preserve own resources while using the services of others and consuming their resources. One way of preventing selfishness in a MANET is a detection and exclusion mechanism. This project focuses on the detection phase and present different kinds of techniques that can be used to find selfish nodes. The detection mechanisms described are called activity-based overhearing, iterative probing, and unambiguous probing.

Existing approaches represents how to determine the secure source authentication using TESLA properties and this authentication used for mobile adhoc networks to route the path using AODV and DSR algorithms in an efficient way without any inconsistency. In this paper, we present complete security system for routing control messages through QOS routing protocols in both security and performance. Malicious node identification is performed using QOS constraints.

II. PROBLEM DEFINITION

In wireless networks, signals are transmitted via open and shared media. With out protection, anyone in the transmission range of the sender can intercept the sender’s signal. Therefore, wireless communications are inherently less secure than their wired counterparts. Furthermore, wireless devices usually have limited bandwidth, storage space, and processing capacities. It is harder to reinforce security in wireless networks than in wired networks.Compared with WLANs, the security management in wireless ad hoc networks is much tougher due to the following characteristics.

- **Resource Constraints:** The wireless devices usually have limited bandwidth, memory and processing power. This means costly security solutions may not be affordable in wireless ad hoc networks.
- **Unreliable Communications:** The shared-medium nature and unstable channel quality of wireless links may result in high packet-loss rate and re-routing instability, which is a common

phenomenon that leads to throughput drops in multi-hop networks. This implies that the security solution in wireless ad hoc networks cannot rely on reliable communication.

- **Node mobility and dynamic topology:** The network topology of wireless adhoc network may change rapidly and unpredictably over time, since the connectivity among the nodes may vary with time due to node departures, node arrivals, and the mobility of nodes. This emphasizes the need for secure solutions to be adaptive to dynamic topology.

Scalability: Due to the limited memory and processing power on mobile devices, the scalability is a key problem when we consider a large network size. Networks of 10,000 or even 100,000 nodes are envisioned, and scalability is one of the major design concerns.

III. RELATED WORK

The existing SRPs for ad hoc networks can be divided into two categories: in terms of how an SRP is secured and what types of attacks it can defend. In the first category, the commonly used method is to establish a security association between the source and destination nodes so that the on-demand routing protocols, such as AODV, DSR, and DSDV, can be secured. There is an SRP called Ariadne based on DSR that uses efficient symmetric cryptography. Ming Yu- Kin K.Leung [5] et al, A Trustworthines Based QoS Routing Protocol For Wireless Ad Hoc Networks was proposed QOs protocols for routing algorithms. Routing messages are authenticated by shared secrets between each pair of nodes. The broadcast authentication scheme used in Ariadne is TESLA, which requires loose time synchronization. In, the authors proposed a proactive SRP, called SEAD, based on DSDV by using one-way hash chains to provide authentication to defend attacks that modify routing information broadcast and replay attacks but not wormhole attack. M. Yu, S. Kulkarni, and P. Lau[6] et al, A new secure routing protocol to defend Byzantine attacks for ad hoc networks was proposed to securely send data using standardized protocols. In order to secure on-demand protocols such as AODV and DSR, the authors developed an authenticated routing protocol, called ARAN, by using digital signature to provide end-to-end authentication, message integrity, and non repudiation. During route discovery, a routing message is signed by a source node and then broadcasted to others.. During route setup, the message is similarly signed twice and unicasted back to the source. Due to its use of double signatures, ARAN can defend most common attacks.

Potlapally, N.R, Ravi, S, Raghunathan. A.,Jha N.K [7], A study of the energy consumption characteristics of cryptographic algorithms and security protocols was proposed for mobile adhoc networks.The accumulated path is protected by an aggregate signature scheme, which is even more expensive than RSA signatures. Few authors have proposed an SRP against Byzantine failures by using source routing and destination acknowledgements. Each packet is authenticated at each node by using MACs based on pair-wise secret keys. Digital signatures are used for initial key setup. Misbehaviors are detected on a per packet basis to defend Byzantine adversaries.

IV. EXISTING SYSTEM

A. Efficient and Secure Source Authentication

This section illustrated with several substantial modifications and improvements to TESLA [5]. One modification allows receivers to authenticate most packets as soon as they arrive. Other modifications improve the scalability of the scheme, reduce the space overhead for multiple instances, increase its resistance to denial-of-service attacks, and more. The security property TESLA guarantees is that the receiver never accepts Mi as an authentic message unless Mi was actually sent by the sender. Note that TESLA does not provide non-repudiation, that is, the receiver cannot convince a third party that the stream arrived from the claimed source.

B. Authenticated Routing for Ad hoc Networks

Securing protocols for mobile ad hoc networks presents unique challenges due to characteristics such as lack of predeployed infrastructure, centralized policy and control. This paper makes a number of contributions to the design of secure ad hoc routing protocols. First, it describes exploits that are possible against ad hoc routing protocols [6]. It shows specifically that two protocols that are under consideration by the IETF for standardization, AODV and DSR, although efficient in terms of network performance, are replete with security flaws. Second, it defines and distinguish the heterogeneous environments that make use of ad hoc routing and differ in their assumed pre-deployment and security requirements. Third, it proposes a secure routing protocol, ARAN that detects and protects against malicious actions by third parties and peers.

C. *Distance Vector Routing Protocol for MANETs*

The design and evaluation of the Secure Efficient Ad hoc Distance vector routing protocol, a secure ad hoc network routing protocol based on the design of the Destination-Sequenced Distance-Vector routing protocol. In order to support use with nodes of limited CPU processing capability, and to guard against DoS attacks in which an attacker attempts to cause other nodes to consume excess network bandwidth or processing time.

SEAD performs well over the range of scenarios they tested, and is robust against multiple uncoordinated attackers creating incorrect routing state in any other node, even in spite of any active attackers or compromised nodes in the network. They present the design and evaluation of a new secure ad hoc network routing protocol using distance vector routing. Their protocol, which we call the SEAD, is robust against multiple uncoordinated attackers creating incorrect routing state in any other node, even in spite of active attackers or compromised nodes in the network. They base the design of SEAD in part on the DSDV. In order to support use of SEAD with nodes of limited CPU processing capability and it uses efficient one-way hash functions and do not use asymmetric cryptographic operations in the protocol. To reduce the number of redundant triggered updates, each node in DSDV tracks, for each destination, the average time between when the node receives the first update for some new sequence number for that destination, and when it receives the best update for that sequence number for it (with the minimum metric among those received with that sequence number); when deciding to send a triggered update, each DSDV node delays any triggered update for a destination for this average weighted settling time, in the hope of only needing to send one triggered update, with the best metric, for that sequence number. SEAD does not use such a delay, in order to prevent attacks from nodes that might maliciously not use the delay.

D. A Secure On-Demand Routing Protocol for Ad Hoc Networks

Two contributions are proposed to the area of secure routing protocols for ad hoc networks. First, they give a model for the types of attacks possible in such a system, and they describe several new attacks on ad hoc network routing protocols. Second, they present the design and performance evaluation of a new on-demand secure ad hoc network routing protocol, called Ariadne, that withstands node compromise and relies only on highly efficient symmetric cryptography. Relative to previous work in securing ad hoc network routing protocols, Ariadne is more secure, more efficient, or more general (e.g., Ariadne does not require a trusted hardware and does not require powerful processors).

V. PROPOSED SYSTEM

This section illustrates A complete security solution should include three components of prevention, detection, and reaction, and provides security properties of authentication, confidentiality, non-repudiation, integrity, and availability. The routing control messages are secured by using both public and shared keys, which can be generated on-demand and maintained dynamically.

A. Complete Security system for message exchange

The routing attacks like black hole, gray hole, worm hole, rushing attack, DOS attack, flooding etc; can become hazardous to the network-layer protocol which needs to be protected. Further the malicious nodes may deny forwarding packets properly even they have found to be genuine during the routing discovery phase. A malicious node can pretend to join the routing correctly but later goes on ignoring all the packets that pass through it rather than forwarding them. This attack is called black hole, or selective forward of some packets is known as grey hole attack. The basic solution needed to resolve these types of problems is to make sure that every node in a network forwards packets to its destination properly. To ensure this kind of security to network layer in MANETS a new secure approach which uses a simple acknowledgement approach and principle of flow conservation is proposed here. As a part of this research work we have tried the same approach with AODV protocol and it has identified two of the attacks namely message tampering and packet eavesdropping. Here, in this proposed work the same approach has been tested to identify more than two attacks in a network without the use of protocol.

The message exchange mechanism also provides a way to detect against routing protocols, particularly the most difficult internal attacks. The routing metrics are obtained by combining the requirements on the trustworthiness of the nodes in the network and the QoS of the proposed secure QoS routing protocol in both security and performance. Its also to be extent using the cryptographic technique called Elliptic Curve Cryptography and also to perform secure data transfer using Adhoc. For these reasons, we propose a new secure Qos routing protocol. First, it is able to detect the difficult internal attacks, including Byzantine attacks by identifying the malicious node. Second, the results on the message verification conducted by a Node is used to build a trustworthiness repository by the node on its neighboring nodes that deliver the message. Third, the trustworthiness is incorporated into the routing metrics, which contains the QoS requirement on the links along a route, such as packet delay and link quality. Secure Route Discovery, Secure Route Setup and maintenance are kept as an integral part of the project.

In Fig 5.1 shows, the sender node module generates the front end and asks the user to enter the message. The user enters the messages or browses the file to be sent and clicks on send button. The counter Cpkt gets incremented every time a packet is sent and the time will be the start time. According to the data format only 48 bytes are sent at a time. If the message is longer than 48 bytes then it is divided into packets each of 48bytes. For maintaining intact security in the algorithm a semantic mechanism like one-way hash code generation to generate the hash code for the message is used.

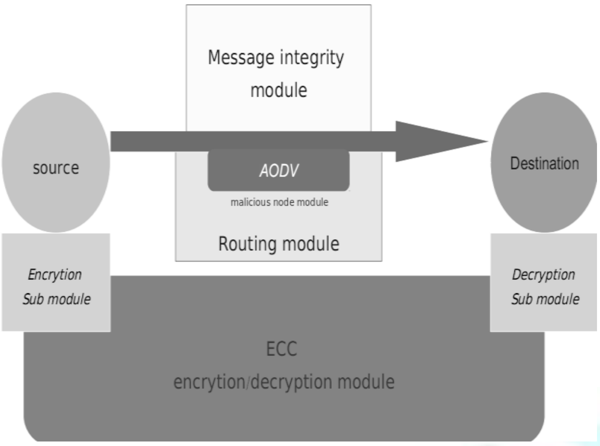

Fig.5.1: Architecture of Complete Security System

A hash function is an algorithm that turns messages or text into a fixed string of digits, usually for security or data management purposes. The "one way" means that it's nearly impossible to derive the original text from the string. A one-way hash function is used to create digital signatures, which in turn identify and authenticate the sender and message of a digitally distributed message. The data to be encoded is often called the "message", and the hash value is sometimes called the message digest or simply digests. Sender module then prepares the data frame appending the necessary fields namely source address, destination address, hash code and data to be sent. Then the data packets will be sent to nearest intermediate nodes. On receiving the message at the intermediate node, a choice will be made available at the nodes module to alter or not to alter the data and the intermediate node behaves accordingly. Then the intermediate node finds the destination address in the data frame and forwards data to it. Once the receiver receives the message, it extracts the fields from the data frame. These extracted fields are displayed on to the front end generated by the receiver module. The receiver also computes the hash code for the message received using the same hash function that was used at the sender. The receiver compares the hash code that was extracted from the data frame with the hash code that it has generated. An accidental or intentional change to the data will change the hash value. If the hash codes match, then the acknowledgement packet sent back to the sender through the intermediate node consists of "ACK". The acknowledgement packet sent back to the sender through the intermediate node consists of "Confidentiality Lost". At the sender node, the sender waits for the acknowledgement packet to reach. Once it receives the acknowledgement packet it computes the time taken for this acknowledgement to reach. If the total transmission time taken is more than the pre-specified interval of 20 ms, it discards the corresponding data packet and accounts it as lost data packet, thereby incrementing the Cmiss counter. Else it checks for the contents of acknowledgement field. If the ratio of 20%, then the intermediate node is said to be misbehaving and a new field "Confidentiality Lost" is built in to the acknowledgement frame. In such a case, sender switches to an alternate intermediate node for the future sessions. Otherwise another new field "ACK" is built in to the acknowledgement frame. In this case the intermediate node is considered to be behaving as expected and transmission is continued with the same intermediate node. Such intermediate nodes can be called genuine nodes. Simultaneously malicious nodes are identified and prevented which launch attacks. The algorithm mainly identifies four attacks parallelly namely packet eavesdropping, message tampering, black hole attack and gray hole attack. This reason makes the algorithm more robust in nature against other approaches. Even it can also be extended to few more network layer attacks

B. Malicious Node identification

a. Adding Malicious node to AODV

The approaches are used to trying to define if the node is malicious or not. In mypacket.cc after add the following line for link the TCL. Now we will do some work in TCL to set a malicious node. Use a TCL script with the following parameter we first set simulation environment. We are going to deploy 500 nodes, in 1000x500 sqm area, simulation time is 500 seconds. And we are using 802.15.4 MAC/PHY and interface queue is 100. We also set simulator and files to trace the simulation. We have set malicious node but we did not tell malicious node what to do. As it is known, rt_resolve (Packet *p) function is used to select next hop node when routing data packets. So, we tell malicious node just drop any packet when it receives.

b. Preventing Selfish Node

There are two approaches of dealing with selfish nodes. The first approach tries to give a motivation for participating in the network function. A typical system representing this approach is Nuglets by Hubeaux et al. The authors suggest to introduce a virtual currency called Nuglets that is earned by relaying foreign traffic and spent by sending own traffic. The major drawback of this approach is the demand for trusted hardware to secure the currency. There are arguments that tamper-resistant devices in general might be next to impossible to be realized. A similar approach without the need of tamper proof hardware has been suggested by Zhong et al. in. There exist also other unresolved problems with virtual currencies, like e.g. nodes may starve at the edge of the network because no one needs them for forwarding etc. Most of the existing work in this field concentrates on the second approach: detecting and excluding misbehaving nodes. The first to propose a solution to the problem of selfish (or as they call it"misbehaving") nodes in an ad hoc network were Marti, Giuli, Lai and Baker in. Their system uses a watchdog that monitors the neighboring nodes to check if they actually relay the data the way they should do. Then a component called path rater will try to prevent paths which contain such misbehaving nodes. As they indicate in their paper, their detection mechanism has a number of severe drawbacks. Relying only on overhearing transmissions in promiscuous mode may fail due to a number of reasons. In case of sensor failure, nodes may be falsely accused of misbehavior. The second drawback is that selfish nodes profit from being recognized as misbehaving. The paths in the network are then routed around them, but there is no exclusion from service. We will later present more advanced sensors that will allow a better detection of selfish nodes.

The distributed intrusion detection system for MANETs that consists of the local components ”data collection”, ”detection” and ”response” and of the global components ”cooperative detection” and ”global response”. Whereas their architecture is very promising and similar to the one we use in our project, they neglect the aspect how their local data collection should find out on incidents like dropped packets, concealed links, etc. Another system called,”COllaborative REputation Mechanism” or CORE. It is similar to the distributed by Zhang et al. and consists of local observations that are combined and distributed to calculate a reputation value for each node. Based on this reputation, nodes are allowed to participate in the network or are excluded. In their work, the authors specify in detail how the different nodes should cooperate to combine the local reputation values to a global reputation and how they should react to negative reputations of nodes.

The probing techniques described so far face a serious problem: probing cannot unambiguously detect a selfish node. Even worse, the standard probing described allows a malicious node to make another arbitrary node look selfish. Our iterative-probing can narrow the potential adversary nodes down to two nodes. In order to clearly identify one of these nodes as being responsible for the dropped data packets, we can combine the iterative probing with overhearing. The attacks explanation is as follows:

Packet eavesdropping: In mobile ad hoc networks since nodes can move arbitrarily the network topology which is typically multi hop can change frequently and unpredictably resulting in route changes, frequent network partitions and possibly packet losses.

Message tampering: The intermediate nodes sometimes don’t follow the network security principle of integrity. They will tend to tamper the data that has been sent either by deleting some bytes or by adding few bytes to it.

- **Black hole attack:** In this attack a misbehaving node drops all the packets that it receives instead of normally forwarding those. The routing message exchange is only one part of the network-layer protocol which needs to be protected. It is still possible that malicious nodes deny forwarding packets correctly even they have acted correctly during the routing discovery phase.

- **Gray hole attack*:*** A variation of the black hole attack is the gray hole attack. This attack when launched by the intermediate nodes selectively eaves drop the packets I.e. 50% of the packets, instead of forwarding all. This attack is identified if the ratio (Cmiss/Cpkt)>0.2 and (Cmiss/Cpkt) = 0.5, then we can say half of the packets that have been sent are eaves dropped by the malicious node.

VI. ELLIPTIC CURVE CRYPTOGRAPHY

The mathematical definition of the elliptic curves we will work with in the following. Then, the polynomial equation is:

E: y2 + xy = x3 + ax2 + b;

With coe_cients a; b 2 F2m together with the point at in_nity O de_ne an elliptic curve over F2m. Let us ask for solutions (x; y) with x; y 2 F2m. Such a solution is called point on the elliptic curve E.

A .Group Law in Elliptic Curve

For the purpose of cryptography, an elliptic curve can be thought of as being given by an affine equation of the form y2 = x3 + *ax* + *b*, where *a* and *b* are elements of a finite field with pn elements, where *p* is a prime larger than 3. (The equation over binary and ternary fields looks slightly different.)

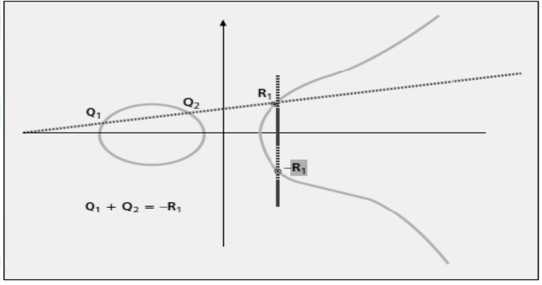

Fig.6.1: Group Law in Elliptic Curve

The set of points on the curve is the collection of ordered pairs (x, y) with coordinates in the field and such that x and y satisfy the relation given by the equation defining the curve, plus an extra point that is said to be *at infinity*. The set of points on an elliptic curve with coordinates in a finite field also form a group, and the operation is as follows: to add two points on the curve **Q**1 and **Q**2 together, pass a straight line through them and look for the third point of intersection with the curve, **R**1. Then reflect the point **R**1 over the x-axis to get –**R**1, the sum of **Q**1 and **Q**2. Thus, **Q**1 + **Q**2 = –**R**1. The idea behind this group operation is that the three points **Q**1, **Q**2, and **R**1 lie on a common straight line, and the points that form the intersection of a function with the curve are considered to add up to be zero

VII. SIMULATION RESULTS

This section shows the simulation results of malicious node identification for mobile adhoc networks.In fig 7.1 shows the effect of a single selfish node identified among the number of nodes deployed into the network. The graph illustrates between throughput of receiving number of packets (no of packets=TTL) and time taken to simulate a packet in seconds. In this Fig 7.2 shows the throughput of network in the absence of selfish nodes in the mobile adhoc networks. The throughput can be achieved higher performance compared to the presence of selfish nodes in the network much better results in an efficient with low overhead and the throughput can be increased as shown in Fig.7.2.

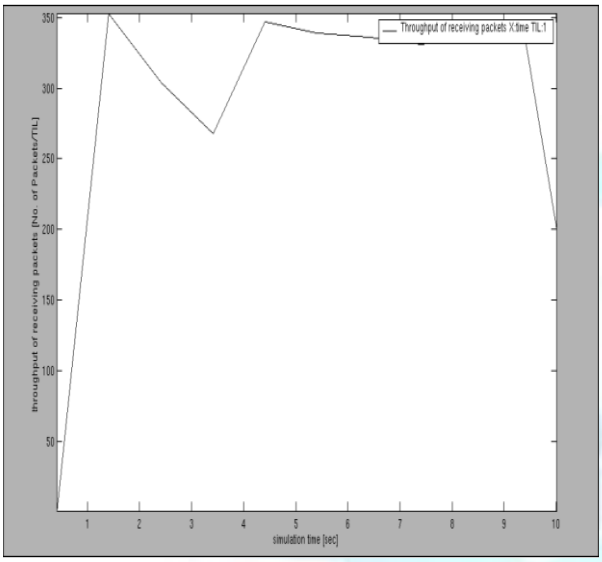

Fig 7.1 Effect of a single selfish node on network throughput

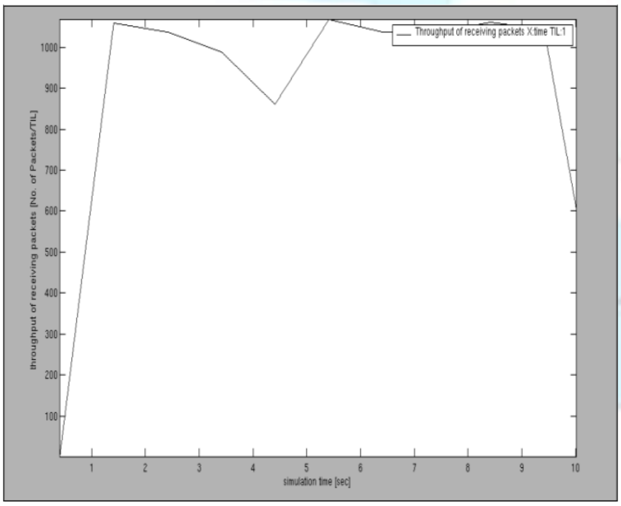

Fig. 7.2 Throughput of network in the absence of selfish nodes

VIII. CONCLUSION

In mobile ad hoc networks, protecting the network layer from attacks is an important research topic in wireless security. This paper describes a robust scheme for network-layer security solution in ad hoc networks, which protects both, routing and packet forwarding functionalities without the context of any data forwarding protocol. This approach tackles the issue in an efficient manner since four attacks have been identified parallelly. The overall idea of this algorithm is to detect malicious nodes launching attacks and misbehaving links to prevent them from communication network. This work explores a robust and a very simple idea, which can be implemented and tested in future for more number of attacks, by increasing the number of nodes in the network. To this end, we have presented an approach, a network-layer security solution against attacks that protects routing and forwarding operations in the network.

IX. FUTURE ENHACEMENT

In the future this project can be enhanced as a potential direction for future work; we are considering measurement of more number of network parameters, to analyze the performance of such a network using the proposed approach.

References

[1] B.S Manoj and C. Siva Ram Murthy, “Ad Hoc wireless Networks, pp. 86–95.2004.

[2] Klara Nahrstedt, Wenbo He, and Ying Huang,"Guide to Wireless Ad Hoc Networks Architectures and Protocols”, pp. 12-18.2009.

[3] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. Belding Royer , “Authenticated routing for ad hoc networks," IEEE J. Select. Areas Commun., vol. 2, no.1, pp. 1-5.2005.

[4] Ming Yu- Kin K.Leung, “A Trust worthiness Based QoS Routing Protocol For Wireless Ad Hoc Networks”,IEEE Transactions on Wireless Communication s, vol. 8, no.4, pp. 1-12.2009.

[5] M. Yu, S. Kulkarni, and P. Lau , “A new secure routing protocol to defend Byzantine attacks for ad hoc networks," in Proc. IEEE Int. Conf.Networks (ICON’05), vol. 2, pp. 1126-1131, 2009.

[6] Potlapally, N.R.; Ravi, S.; Raghunathan, A.; Jha, N.K.,”A study of the energy consumption characteristics of cryptographic algorithms and security protocols”, IEEE Transactions on Mobile Computing, Volume: 5 Issue:2 pp. 49-59.2009.

[7] Sunil Taneja,Ashwani Kush,Amandeep Makka, "Performance Evaluation of Protocols for Secure Routing over MANET", Proceedings of the 4th National Conference; INDIACom-2010 Computing For Nation Development pp. 586–615.2010.

[8] Y.-C. Hu, A. Perrig, and D. B. Johnson , “Ariadne: a secure on-demand routing protocol for ad hoc networks," in Proc. 8th ACM International Conf. Mobile Computing Networking , pp. 27-34. 2002.

[9] Y.-C. Hu, D. B. Johnson, and A. Perrig, “SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks," in Proc. 4th IEEE Workshop Mobile Computing Syst. Applications, pp. 156-192.2002.