

# Robust And Secured WEP Protocol For Wireless Adhoc Network

Mr. S.M.K.M. Abbas Ahmad<sup>1</sup>, Dr. E.G. Rajan<sup>2</sup>, Dr. A.Govardhan<sup>3</sup>

<sup>1</sup>Associate Professor, Dept. of E.C.E., Hi-Tech College of Engg & Tech, Hyderabad, India, Phone: +919440434385, Email: [smkmabbas@rediffmail.com](mailto:smkmabbas@rediffmail.com)

<sup>2</sup>Director, Sagar Institute of Technology, Hyderabad, India, Phone: +91849164747, Email: [rajaneg@yahoo.co.in](mailto:rajaneg@yahoo.co.in)

<sup>3</sup>Principal, JNT University Engineering College, Jagityal, India, Phone: +919440887733, Email: [govardhan\\_cse@yahoo.co.in](mailto:govardhan_cse@yahoo.co.in)

*Abstract---The WEP protection technique suggested for adhoc network fall short of the objective of data privacy, data integrity, and authentication. Various security standards such as IEEE 802.11i, WPA, IEEE 802.1X were suggested to enhance the security issues in 802.11. Despite their efficiency, these standards do not provide any robustness to the security approach for monitoring of the authentication in a distributed architecture. For the efficient monitoring of the authentication issue in adhoc network, we present a self monitored and trustworthy security approach for wireless adhoc networks. The processing overhead for the suggested approach is evaluated for a distributed adhoc network and the results are promising.*

**Index Terms--self secure, adhoc network, WEP protocol, Trustworthiness, MANET, robust**

## I. INTRODUCTION

Wireless networking grows rapidly because of the human desires for mobility and for freedom from limitation, i.e., from physical connections to communication networks. A mobile adhoc network is a wireless, self-organizing and rapidly deployable network in which neither a wired backbone nor a centralized control exists. The network nodes communicate with one another over scarce wireless channels in a multi-hop fashion. The adhoc network is adaptable to the highly dynamic topology resulted from the mobility of network nodes and the changing propagation conditions. These networks are used in emergency disaster rescue operation, tactical military communication and law enforcement. The commonly used 802.11b MAC protocol includes support for an ad-hoc mode of operation. Such networks are often used in cases of rapid deployment, in places lacking adequate infrastructure, or to facilitate direct communication between nodes when the base station becomes the bottleneck. In some application environments, such as battlefield communications, disaster recovery etc., the wired network is not available and multi-hop wireless networks provide the only feasible means for communication and information access. This kind of network is called Mobile Adhoc Network (MANET). A MANET can be seen as an autonomous system or a multi-hop wireless extension to the Internet. As an autonomous system, it has its own routing protocols and network management mechanisms. As a multi-hop wireless extension, it should provide a flexible and seamless access to the Internet. Recently, because of the rising popularity of multimedia applications and potential commercial usage of MANETs, QoS support in MANETs

has become an unavoidable task. By definition, a mobile adhoc network does not rely on any fixed infrastructure; instead, all networking functions (e.g. routing, mobility management, etc) are performed by the nodes themselves in a self-organizing manner[11]. For this reason, securing mobile adhoc networks is challenging and in some applications this requires modifications with respect to the traditional security solutions for wire line networks. There are two extreme ways to introduce security in mobile adhoc networks: 1) through a single authority domain, where certificates and/or keys are issued by a single authority, typically in the system setup phase or 2) through full self-organization [11], where security does not rely on any trusted authority or fixed server, not even in the system initialization phase. In contrast with conventional networks, mobile adhoc networks usually do not provide on-line access to trusted authorities or to centralize servers [1] and they exhibit frequent partitioning due to link and node failures and to node mobility. For these reasons, traditional security solutions that require on-line trusted authorities or certificate repositories are not well suited for securing adhoc networks [2]. In this paper, we propose a self-monitored key management with trustworthiness that allows users to generate their key pairs, issue certificates, and perform authentication regardless of the network partitions and without any centralized services. A self organizing key management system that allows users to create, store, distribute and revoke their keys without the help of any trusted authority or fixed server is developed.

## II. SECURITY IN ADHOC NETWORK

Security is a fundamental issue that needs resolution before adhoc networks will experience large-scale deployment [9]. For example, some existing routing protocols for mobile adhoc networks may be able to manage the dynamic network topology of mobile adhoc networks, but none of these protocols [8] incorporate mechanisms to prevent, tolerate or defend against attacks from malicious adversaries. Researchers in the adhoc network security field initially focused on secure routing protocols. The focus of these protocols are:

1. To provide a robust routing mechanism against the dynamic topology of MANETs [3].

2. To provide a robust routing mechanism against malicious nodes

#### A. Wired Equivalent Privacy Protocol

The WEP was designed by a group of IEEE volunteer members, aiming at giving some layer of security to wireless networks.

In this section, WEP functioning process is described, which includes mechanisms used to implement security services.

Initially, both of the communication entities share a secret key  $k$ .  $k$  will be used further to encrypt transmitted data [4]. Let  $S$  be a source which sends a message  $M$  to a receiver  $R$ .  $S$  begins by calculating a checksum using the CRC (Cyclic Redundancy Check) algorithm widely used in network protocols. Let us note  $T=(M,CRC)$  the message produced by a simple concatenation of  $M$  and its CRC.

Then,  $S$  encrypts  $T$  using the RC4 algorithm [2]. RC4 is a stream cipher [3]: It generates a keystream  $KS$  using two inputs:

- The key  $k$  shared between  $S$  and  $R$ , which is 40 bits length;
- An Initialization Vector  $iv$ , used principally to minimize probability of feeding RC4 with the same entries (which leads to the same keystream in output).  $KS$  is XORed with  $T$  to produce the cipher text  $C$ . To decrypt  $C$ ,  $R$  needs to reconstruct the same keystream  $KS$  and XOR it with  $C$ , indeed: However, to reproduce  $KS$ ,  $R$  needs to know  $iv$ . In WEP,  $iv$  is concatenated to the cipher text  $C$  before sending it. Note that  $iv$  is sent as clear text, without any kind of encryption. This process ensures:

- Data Privacy: all transmitted data is encrypted and only communication entities can decrypt it;
- Data Integrity and Authentication: the checksum is verified upon receiving the message. Thus, all modifications of the message during its transmission will be detected.

All WEP weaknesses come from four main conception flaws:

- i) The initialization vector is transmitted as clear text. Beside the fact that this weakens the power of encrypting, attackers are in a position to detect every  $iv$  reuse.
- ii) The key is rarely renewed: Key ( $k$ ) updating techniques are completely leaved as implementation details. Thus, manufacturers are free to use the techniques that they find suitable. The worst, an implementation that doesn't plan key renewing is within the norm.
- iii) Data Source Authentication: The WEP has not planed a mechanism to ensure data source authentication. As mentioned above, using CRCs allows attackers to forge their own messages, and send them as coming from a known entity (this hole is called impersonation). Using Message Authentication Code (MAC) would be an efficient solution to this problem. MACs are usually used to guarantee data source authentication.

Another solution is to secure enough privacy mechanism, so that nobody will be able to access the CRC. This is what WEP intended to do but failed to achieve.

iv) Security services are all implemented using only one mechanism [10]. All the security schemes are based upon the strength of the mechanism of data privacy service. Thus, once the privacy of data is broken, all other services, data integrity and access control are directly broken.

### III. SELF MONITORING APPROACH

The main problem of any key based security system is to make each user's key available to others in such a way that its authenticity is verifiable. In mobile adhoc networks, this problem becomes even more difficult to solve because of the absence of centralized services and possible network partitions. More precisely, two users willing to authenticate each other are likely to have access only to a subset of nodes of the network (possibly those in their geographic neighborhood). The best-known approach to the key management problem is based on key certificates.

The self-organizing concept includes two stages

- 1) Key Distribution /Initialization
- 2) Authentication

In an adhoc network, in order for the nodes to communicate, it is essential that each node have the information about the rest of the nodes in the network. In particular, the keys of the nodes that are in its communication range are the most important parameter.

In self-organization [11] method, key distribution is the initial phase, executed in three steps as follows:

Step-1: Creation of Key Pairs: Users locally create their own private key and corresponding key.

Step-2: Key distribution: Depending up on the communication range of the nodes, they find out their nearest neighbors or the nodes that can be reached in one-hop. Once the nodes generate their keys, key distribution takes place. During broadcast period, each user broadcasts its key to all its nearest neighbors or one-hop neighbors. This is a synchronous process i.e. every node does this simultaneously. Now all the users in the network are aware of the keys of their neighbors.

Step-3: Every node receives a set of keys from all its neighbors. A node up on receiving a key from a particular neighbor, issues a certificate comprising the sending node id, key along with its own key. This indicates that the node believes in the sender's identity. That is each node acknowledge back to the sender node with the certificate for the received node key. All the nodes in the network do this simultaneously.

#### A. Authentication:

Each node collects the certificates from all its one-hop neighbors. The Exchanged certificates are saved in the form of a repository table at each node. Consider node  $n$  issued a certificate to node  $m$ . The certificate includes node  $m$ 's id and key  $P_m$  along with node  $n$ 's id and key  $P_n$ . The exchanged certificate gives the authentication of the key received ( $P_m$ ) by presenting the key of node- $m$  which it received, with it' s own key ( $P_n$ ). The authentication of the key is done by the node  $m$  by checking the second field of

the certificate i.e. it's own key(Pm)as received by node-n. That means that node m believes that node n has its valid key and communication can be carried out. The following figure shows the formation of repository tables by the nodes in the network

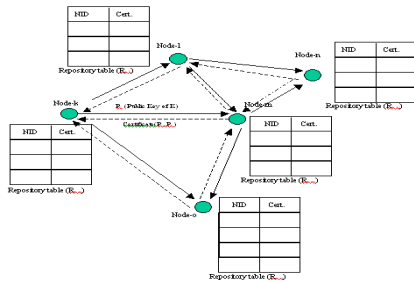


Fig 1: Formation of repository tables

Construction of Updated Certificate Repositories: These neighbors may be same as those, which the node encountered, in the previous beacon period or the node may encounter some new nodes. When a node starts receiving the new certificates, it checks whether its back up repository table contains the similar certificate or not. If it already has similar certificate in its back up non-updated repository table, the newly received certificate is ignored. Like this every new certificate is verified. Scenario when one new node is added to the network after a beacon period is shown in the following figure.

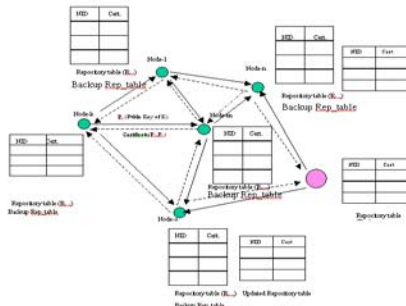


Fig 2: certificate exchange with newly added node

Users can revoke any issued certificate to other users in the instance of distrust in the key binding. Similarly users can also revoke their own certificate if they believe that their private key has been compromised. This key mechanism depend on the reliability of the network parameter and it's trustworthiness.

IV. ROBUSTNESS

Trustiness in Mobile adhoc networks is a important consideration as the nodes rely on the cooperation of all the participating nodes [1]. The more nodes cooperate to transfer traffic, the more powerful a MANET gets. But supporting a MANET is a cost-intensive activity for a mobile node. Detecting routes and forwarding packets consumes local CPU time, memory, network-bandwidth, and most important the energy. Therefore there is a strong motivation for a node to deny packet forwarding to others, while at the same time

using their services to deliver own data. To provide a trustworthiness to the key mechanism in the paper we present a management scheme with key distribution as presented above [6]. The tasks management scheme carries out are, to gather information to classify first-hand experience, to exchange this information and to consider the second-hand information thus received, to update the belief about the behavior of others, which is called the reputation rating, taking into account both first and second-hand information, to classify other nodes based on the reputation rating, and to adapt one's own behavior according to that classification. The management scheme consists of several components that fulfill these tasks [7]. The architecture of the protocol is as shown in following figure.

The components of the protocols are:

- Monitor, Reputation System
- Path Manager, Trust Manager

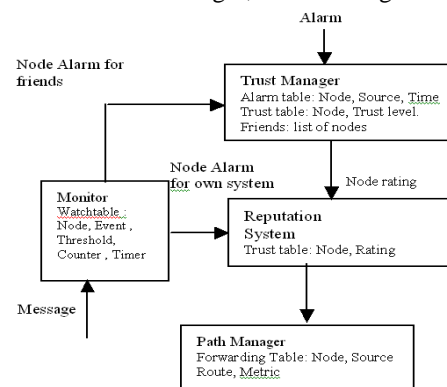


Figure 3: management scheme Architecture within each Node

As shown in Figure 3, the Monitor, the Reputation System, the Path Manager, and the Trust Manager are the components that are present in every node and they are described in detail subsequently.

V. THE MONITOR (NEIGHBORHOOD WATCH)

In a networking environment, the nodes most likely to detect non-compliant behavior are the nodes in the vicinity of the non trusty node and in some case the source and the destination, if they detect unusual behavior or do not get proper responses. One approach to protocol enforcement and detection of damaging behavior (intrusion, misuse of cooperation incentives, denial of service, etc.) suggested here is the equivalent of a 'neighborhood watch', where nodes locally look for deviating nodes. The neighbors of the neighborhood watch can detect deviances by the next node on the source route by either listening to the transmission of the next node or by observing route protocol behavior. By keeping a copy of a packet while listening to the transmission of the next node, any content change can also be detected. In this paper we focused on the detection of observable routing and forwarding misbehavior in DSR. In general, the following types of misbehavior can be indicated: no forwarding (of control messages nor data),

unusual traffic attraction (advertises many very good routes or advertises routes very fast, so they are deemed good routes),  
 route salvaging (i.e. rerouting to avoid a broken link), although no error has been observed,  
 lack of error messages, although an error has been observed,  
 unusually frequent route updates,  
 silent route change (tampering with the message header of either control or data packets).

As a component within each node, the monitor registers these deviations of normal behavior. As soon as a given bad behavior occurs, the reputation system is called.

VI. THE TRUST MANAGER

In an ad hoc environment, trust management has to be distributed and adaptive. This component deals with incoming and outgoing alarm messages. alarm messages are sent by the trust manager of a node to warn others of malicious nodes. Incoming alarms originate from outside friends, whereas the node itself generates outgoing alarms after having experienced, observed or been reported malicious behavior.

A. The Reputation System (Node Rating)

In order to avoid centralized rating, local rating lists and/or black lists are maintained at each node and potentially exchanged with friends. The nodes can include black sheep in the route request to be avoided for routing, which also alarms nodes on the way. Nodes can look up senders in the black list containing the nodes with bad rating before forwarding anything for them. The problem of how to distinguish alleged from proven malicious nodes and thus how to avoid false accusations can be lessened by timeout and subsequent recovery or revocation lists of nodes that have behaved well for a specified period of time.

B. The Path Manager

Once a node i classifies another node j as misbehaving, i isolates j from communications by not using j for routing and forwarding and by not allowing j to use i. This isolation has three purposes. The first is to reduce the effect of misbehavior by depriving the misbehaving node of the opportunity to participate in the network. The second purpose is to serve as an incentive to behave well in order not to be denied service. Finally, the third purpose is to obtain better service by not using misbehaving nodes on the path.

VII. SIMULATION RESULTS

The proposed self-monitored key management scheme is implemented on an ad hoc network. The network is created with randomly distributed nodes. Network is considered with the following properties:

Distribution	: Random
Number of Nodes	: 17
Region	: 280 x 300 units
Communication Range	: 80 units
Mobility	: Static
MAC	: 802.11
Packet Size	: 61 bits
Weight (w)	: 0.1
Trustworthy Threshold (t)	: 0.75
Node status threshold (r)	: 0.5

Several adhoc networks are tested for various cases of network load. Even variable number of nodes is taken into account. Performance of both threshold based cryptography and self monitored approach are tested. The three analysis factors mentioned in the previous section are evaluated in both the cases.

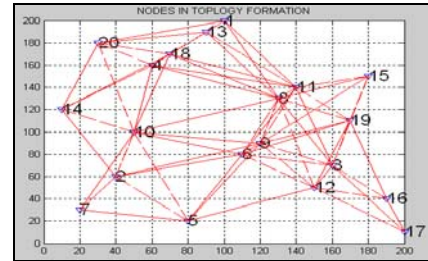


Fig 5: Simulated network with the stated specifications

Case 1: With No Add-on nodes ,Source node:18  
 Destination node:12, Route taken for communication from source to destination: 18 → 4 → 6 → 17 → 12

1) Fig 5 shows a dynamic ad hoc network with 20 nodes and 8 misbehaving nodes distributed randomly.

2) The fig 6 shows the performance of DSR with trust route protocol for the above randomly distributed network We have chosen 7 as source node and 15 as destination node. Misbehaving nodes are indicated by round circles .The black dotted line shows the optimum path that has been selected to reach the destination. The fig clearly shows that trust route protocol is able to cope with misbehavior in mobile ad hoc networks thus making network function for normal nodes when other nodes don't route and forward correctly. The protocol is integrated with modified Bayesian approach to decide whether node is misbehaving or not

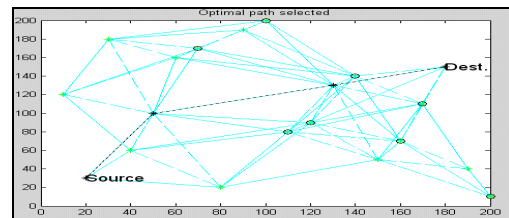


Fig 6: DSR with trust route performance for the randomly distributed network shown in fig: 2

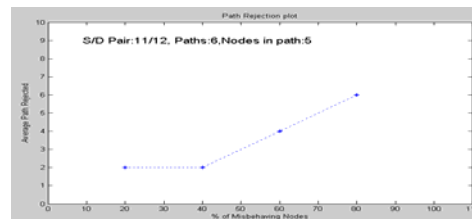


Figure 7: Average path rejections wrt. Misbehaving nodes

The average rejected paths increases if percentage of malicious nodes increases but with the use of RMP average paths rejected remains constant even if the percentage of malicious nodes increases to 40%.

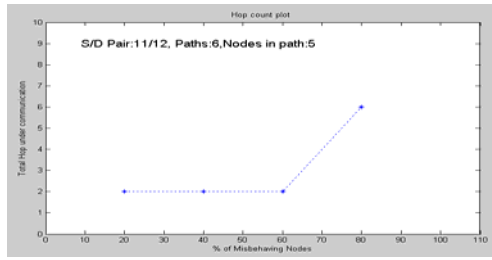


Figure 8. Total Hops under communication w.r.t. Percentage of misbehavior plot

The number of rejected path from the source to destination increases as percentage of misbehaving nodes increases hence the number of hop counts required for communication also increases. The total hop counts for communication remains constant with the use of RMP (Route Management protocol) even if percentage of malicious nodes increases to 60%.

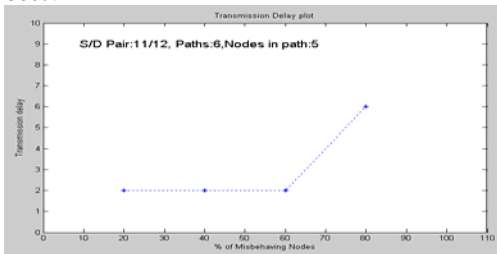


Figure 9: Transmission Delay versus % Misbehavior plot  
The packet transmission delay increases with the increase in percentage of malicious nodes but with use of RMP (Route Management Protocol) the transmission delay remains constant even if the percentage of malicious nodes increases to 60%

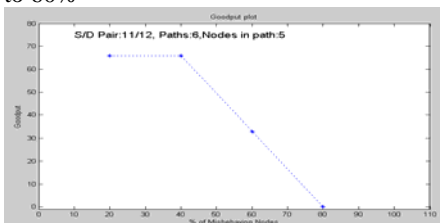


Figure 10: Goodput plot for the network  
Observation:

% Misbehaving Nodes	20%	40%	60%	80%
No. of Rejected path	2	2	4	6
Total Hops under communication	2	2	2	6
Transmission delay in seconds	2	2	2	6
% Goodput	66.67	66.67	33.33	0

VIII. CONCLUSION

In this work, the problem of key management in mobile adhoc networks is addressed. A fully self-monitored key management system for mobile adhoc networks is developed and it is observed that two users in a mobile ad hoc network can perform key authentication based only on their local information, even if security is performed in a self-monitored way, it is shown that with a simple local repository construction algorithm and a small communication overhead,

the system achieves high performance on a wide range of certificate graphs; it is also shown that nodes can have mobility to facilitate authentication and to detect inconsistent and false certificates. An important feature of this scheme is that key authentication is still possible even when the network is partitioned and nodes can communicate with only a subset of other nodes. In this method the involvement of all the nodes are required only when their key pairs are created and for issuing and revoking certificates; all other operations including certificate exchange and construction of certificate repositories are self monitored. it is concluded that node with RMP can sustain the network with efficient data transmission for 50% of misbehaving node.

REFERENCES

- [1] Andreas Pfitzmann, Birgit Pfitzmann, Matheas Schunter, Michael Waidner, "Trusting Mobile User Devices and Security Modules", Information Infrastructure for virtual environment, IEEE, 1997.
- [2] Lidong Zhou and Zygmunt J. Hass, "Securing Ad-hoc Networks", IEEE network, Nov/Dec- 1999.
- [3] Panagiotis Papadimitratos and Zygmunt J. Hass, "Secured Routing for Mobile Adhoc Networks", SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002).
- [4] N. Asokan and P.Ginzhoorg, Chuk Yang Seng, "Key Agreement in Adhoc Networks", presentation.
- [5] David B. Johnson, "Routing in Adhoc Networks of Mobile Hosts", Computer Science Department Carnegie Mellon University Pittsburgh IEEE- 1995.
- [6] Emre Saym & Albert Levi, "Open Trust Scheme For Adhoc Networks", 2006.
- [7] Nancy C. Roberts, Raymond Trevor Bradly, "Research Methodology or New Public Management Network workshop in Siena, Italy July 28-30, 1999.
- [8] Seimg Yi, Prasad Naldurg, Robin Kravets, "A Security- Aware Routing Protocol for Wireless Adhoc Networks", University of Illinois at Urbana-Champaign Urbana, IL 61801.
- [9] Anne Vanhala, "Security in Adhoc Networks", Research seminar on Security in Distributed Systems University of Helsinki.
- [10] Frank Stajano and Ross Anderson, "The Resurrecting Ducklin- Security Protocols, 7<sup>th</sup> International Workshop Proceedings Lecture Notes in Computer Science, 1999.
- [11] Ljubica BlaZevit, Levente Buttyan, Srdjan tapkun, Silvia Giordano, Jean-Pierre Hubaux, and Jean-Yves Le Boudec, "Self-Organization in Mobile Adhoc Network: The Approach of Terminodes", IEEE Communication Magazine, June 2001.