Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 1, January 2014, pg.366 – 373

RESEARCH ARTICLE

DATA ENCRYPTION WITH FRIEND BASED ROUTING TO ESTABLISH SECURITY IN MANET

SHARMILA.G[*1]
M.Tech Student
Department of Computer Science and Engineering
PRIST University Pondicherry, India.
sharmi.deep@gmail.com

J.R.THRESPHINE[*2]
Assistant professor
Department of Computer Science and Engineering,
PRIST University Pondicherry, India.
jrthresphine7@gmail.com

ABSTRACT

A mobile ad-hoc network is an infrastructure less network with self-configuring mobile nodes connected by wireless. To provide more security in MANET routing of data is done through the friends present in the network. The data is being encrypted and then it is routed through the friend list. The malicious nodes are being detected and isolated from the network by the challenge process.

KEYWORDS: *MANTEs; AODV; Encryption; Decryption*

I. INTRODUCTION

Mobile ad-hoc networks do not have any rely on any fixed infrastructure and communicates in organized way. Security is an essential component for basic network functions which include packet forwarding, network management and routing. The nodes in the network act as a router that discover and maintain routes to other nodes in the networks. They communicate using a wireless communication link e.g. a Wireless LAN (WLAN) adapter (IEEE 802.11). These networks are subject to frequent link breaks which also lead to a constantly changing network topology. Due to the specific characteristics of the wireless channel, the network capacity is relatively small. Hence, to be able to use MANETs with many nodes, very effective and resource efficient protocols are needed.

Since the nodes communicate over an air interface, security becomes a very important issue. Compared to a wired link, the wireless link can be intercepted or disrupted by an attacker much more easily, since it is freely accessible and not protected at all. n addition, the constantly changing topology makes it hard to determine which node really left the network, just changed the location, or has been intercepted or blocked. Therefore, mechanisms and protocols have to be developed to secure MANETs. This especially becomes relevant for a commercial use of this technology, since customers expect a high quality service which is trustworthy and reliable. Because of the changing topology special routing protocols have been proposed to face the routing problem in MANETs. Since routing is a basic service in such a network, which is prerequisite for other services, it has to be reliable and trtworthy.following the example. Some components, such as multi-leveled equations, graphics, and tables are not prescribed, although the various table text styles are provided. Attacks in MANET are divided into two types namely active attack and passive attacks. In passive attack the intruder is undetected and hacks the message from the transmitted message. Eaves dropping and traffic analysis belongs to the passive attacks. In active attack the intruder can be detected and affect the communication by changing the data that is sent to the receiver in the network. The important security challenges in MANETS are as follows.

1) The medium is air; hence the network can be tapped easily.
2) The wireless medium has only limited capacity and needs more schemes for fewer networks overhead.
3) The network is dynamic in nature hence self-healing algorithms and self-configuration should be designed in order to detect the security attacks.

II. RELATED WORKS

A. Security in Mobile Ad hoc Networks

The security of ad hoc networks can be based on protection in the link or network layer. In some ad-hoc solutions, the link layer offers strong security services for protecting confidentiality and authenticity, in which case all of the security requirements need not be addressed in the network or upper layers. For providing secure communication in Wireless ad hoc network; there are two ways: (1) Using the multiple paths available in between the two nodes. (2) Using the cryptographic methods to secure the communication in between two nodes.

In first approach all the multiple paths between two nodes need to be node-disjoint. Multipath routing allows building and use of multiple paths for routing between a source-destination pair. Multipath routing can provide a range of benefits like bandwidth aggregation, minimizing end-to-end delay, increasing fault tolerance, enhancing reliability, load balancing, and so on. This approach is cost effective as it does not include any computation or transmission overhead and hardly inject delay in the network. But it does not ensure a certain level of security as there are not always multiple paths between two end nodes.

The second approach is security consideration where it provides optimal security but with the price of too much computation and transmission cost as well as time delay. Since all the nodes in the adhoc network collaborate to forward the data, the wireless channel is prone to various types of attacks. Therefore implementing security is of prime importance in such networks. The ultimate goal of the security solutions for MANETS is to provide security services such as authentication, confidentiality,

integrity, anonymity, and availability to mobile users. Multi-path routing protocols need to be properly enhanced with cryptographic means which will guarantee the integrity of a routing path and the authenticity of the participating nodes.

Authenticity and integrity of routing information are often handled in parallel, if public key cryptosystems are in use, since digital signatures are applied for both confirming the origin of the data and its integrity. Without any integrity protection the attacker is able to destroy messages, manipulate packet headers or even generate false traffic so that the actions cannot be distinguished from hardware or network failures. Authenticity of the routing data is essential so that nodes can confirm the source of new or changed routing information. If authenticity is not guaranteed, the adversary could perform impersonation attacks, divert traffic to arbitrary destinations or even scramble the routing fabric so that connectivity is severely broken in the ad hoc network. In worst case the attacker can perform his actions and leave the network without being regarded as a malicious party.

B. AODV Routing protocol for Ad-Hoc Networks

There are two types of routing protocols which are reactive and proactive. In reactive routing protocols the routes are created only when source wants to send data to destination whereas proactive routing protocols are table driven. Being a reactive routing protocol AODV uses traditional routing tables, one entry per destination and sequence numbers are used to determine whether routing information is up-to-date and to prevent routing loops. The maintenance of time-based states is an important feature of AODV which means that a routing entry which is not recently used is expired. The neighbours are notified in case of route breakage. The discovery of the route from source to destination is based on query and reply cycles and intermediate nodes store the route information in the form of route table entries along the route. Control messages used for the discovery and breakage of route are as follows:

(1) Route Request Message (RREQ)

(2) Route Reply Message (RREP)

(3) Route Error Message (RERR)

(4) HELLO Messages.

A route request packet is flooded through the network when a route is not available for the destination from source. On having a valid route to the destination or if the node is destination, a RREP message is sent to the source by the node. The neighborhood nodes are monitored. When a route that is active is lost, the neighborhood nodes are notified by route error message (RERR) on both sides of link. The HELLO messages are broadcasted in order to know neighborhood nodes. The neighborhood nodes are directly communicated. In AODV, HELLO messages are broadcasted in order to inform the neighbors about the activation of the link. These messages are not broadcasted because of short time to live (TTL) with a value equal to one.

III. FACES PROTOCOL WITH DATA ENCRYPTION

Friend Based routing using challenges to provide security in MANETS is a hybrid protocol. FACES provides authentication of the nodes present in the network. This protocol provides secure routing with data encryption in order to enhance more security in the network. No central authority is needed. It signifies the mistrust of the nodes that are not being used in the

network. The malicious nodes can be detected in the network with less time and network overhead. The protocol contains two types of list namely the unauthenticated list and friend list. The authentication is provided based on the challenge procedure.

A. FACES Algorithm Description

The idea of this scheme is taken from the real life friend scenarios. The people in a group or community are stranger to each other initially, till they become friends and then communication take place between them. In the same way when the network is newly created each node is stranger to each other and takes time for secure information. Tasks are being completed by trusting one another unconditionally and their trust level increases based on the successful task completions.

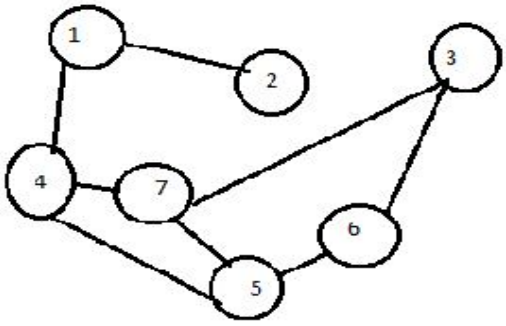

Figure 1. Network of friends in a community

The following section defines the different stages used in the protocol in detail.

1. Nodes Configuration.
2. Neighbor Discovery.
3. Challenge its neighbor.
4. Encryption of data.
5. Routing the encrypted data.

The friend list and the unauthentication list are being created after performing the challenge process.

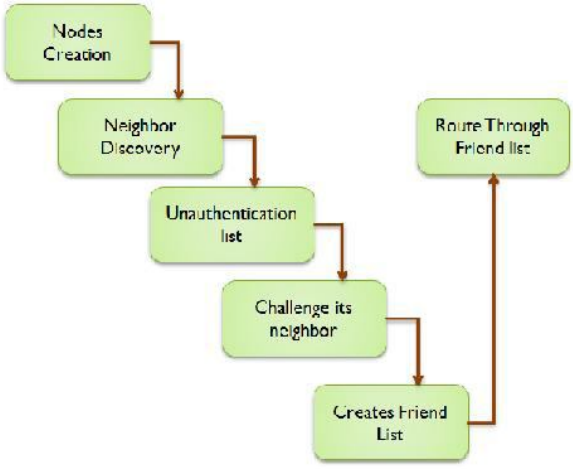

Figure 2. Architecture of the protocol

- Node Creation includes creation of 21 nodes in the network. The topology used is logical topology since all nodes are dynamic in a wireless environment. Flat grid topography is used in this protocol. The energy reception power, idle power and sensing power are being configured. AODV routing protocol is being used.
- Neighbor Discover provides the neighbors for each node that are being present in the network .The neighbors are discovered based on the distance of that particular node. The nodes that are being present below the distance value of 200 in the network are taken as the neighbor of that current node.
- The unauthentication list neighbor nodes in a newly initialized network, this is because in a newly created network each node is stranger to each other. The nodes present in this list are taken as the malicious nodes that perform any malicious activities in the network.
- The friend list is being created to place the friend nodes in the list. Based on the success of the challenge, the nodes are being kept in this list.

B. Challenge its neighbors

Challenge is the process where the nodes prove its integrity and honesty. The main aim is to provide the authentication of the nodes. Challenge is the biggest random prime number that is being generated during the simulation. Initially each node in the network is initialized with two random prime numbers that are secret to that particular node. Challenge is denoted as ”n”. The challenge encryption takes place in the source node. The random prime numbers generated for each node is denoted by x and y respectively. The encryption of the challenge takes place as follows

Encrypted challenge = n+(x, y).

The receiver node receives the encrypted challenge and decrypts the value to obtain the challenge value. The random prime number for receiver node be “a” and “b” respectively the original challenge value is obtained using the decryption method. The decryption takes place in the following manner.

Challenge = (a ^ b) mod n

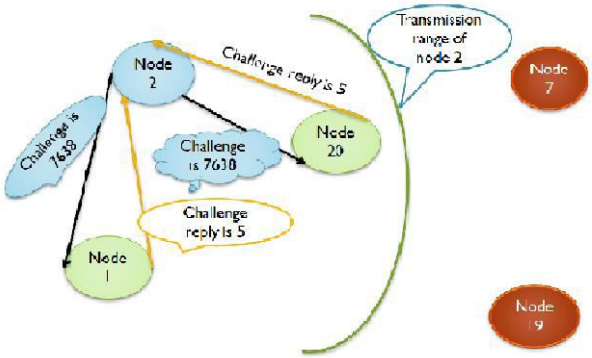

Figure 3. Challenge Process

C. Encryption of data and routing through friends.

- In order to provide more security the data is being encrypted and it is being routed through the nodes in the friends list. .
- The encryption algorithm used in this protocol is Caesar Cipher method such as Vignere cipher. In this encryption method the alphabets are being changed to numbers according to the following scheme A=0, B=1…Z=25.
- Encryption of a letter by a shift n can be described mathematically as,
  En (x) =(x+n) mod 26
- Decryption can be done by the following way.
  Dn(x) =(x-n) mod 26
- Routing is done using the AODV protocol. Routing of data is done based on the on-demand process. Challenges and the friend process are being done in periodic manner, so the protocol is said to be a hybrid protocol.
- Data encryption with friend based routing enhances more security when it is compared with the existing protocol FACES. The protocol reduces the network overhead and the malicious nodes are being detected in the network easily.

IV. RESULT

A. NS -2 Simulators

Ns-2 is a discrete event simulator targeted at networking research. It provides substantial support for simulation of TCP, routing and multicast protocols over wired and wire-less networks. It consists of two simulation tools. The net-work simulator (ns) contains all commonly used IP proto-cols. The network animator (nam) is use to visualize the simulations.Ns-2 fully simulates a layered network from the physical radio transmission channel to high-level applications. Version 2 is the most recent version of ns (ns-2). The simulator was originally developed by the University of Cal-farina at Berkeley and VINT project the simulator was recently extended to provide simulation support for ad hoc network by Carnegie Mellon University (CMU Monarch Project homepage, 1999). The ns-2 simulator has several features that make it suitable for our simulations. A network environment for ad-hoc networks, Wireless channel modules (e.g.802.11), Routing along multiple paths, Mo-bile hosts for wireless cellular networks. Ns-2 is an object-oriented simulator written in C++ and OTcl. The simulator supports a class hierarchy in C++ and a similar class hierarchy within the OTcl interpreter. There is a one-to-one correspondence between a class in the interpreted hierarchy and one in the compile hierarchy. The reason to use two different programming languages is that OTcl is suitable for the pro-grams and configurations that demand frequent and fast change while C++ is suitable for the programs that have high demand in speed. Ns-2 is highly extensible. It not only sup-ports most commonly used IP protocols but also allows the users to extend or implement their own protocols. It also provides powerful trace functionalities, which are very important in our project since various information need to be logged for analysis. The full source code of ns-2 can be downloaded and compiled for multiple platforms such as UNIX, Windows and Cygwin.

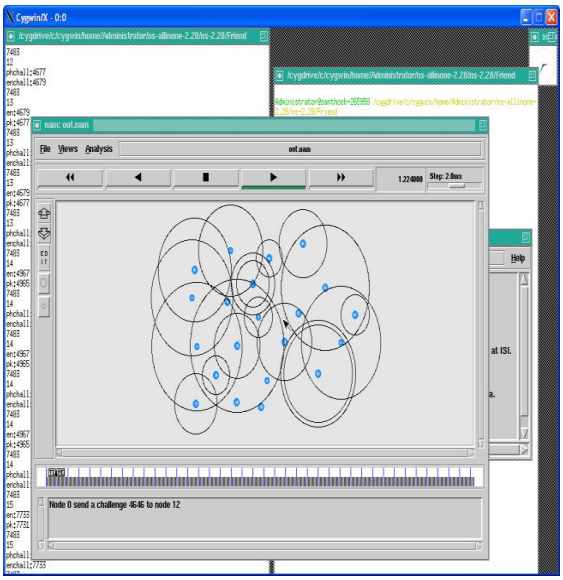

Figure 4. Challenge its neighbor nodes.

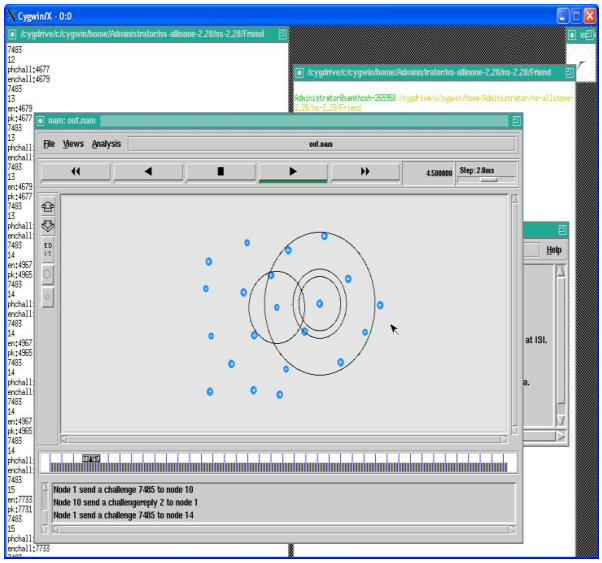

Figure 5. Routing of data

V. CONCLUSION AND FUTURE WORK

The absence of the need of promiscuous mode in the mobile nodes, the network has to bear a lot less overhead as compared to other secure routing schemes. The friends sharing scheme turns out to be an efficient mechanism to spread information about trusted nodes effectively in the system. Since the algorithm does not rely on any scheme to spread information about misbehaving nodes, the chances of grudge wars taking place in the network are zilch. The maliciousness of a node is on the sole discretion of a particular node, which it determines through challenges. Challenges turn out to be efficient mechanism to authenticate nodes because the malicious nodes cannot differentiate between a packet that is meant for a challenge and the one meant for normal data routing. This provides an inherent security to the network and the malicious nodes are easily exposed. In our protocol, we use challenges to authenticate any node compared to the other security protocols that use multipath routing and overhear the neighbor activities. To make a decision that a node is malicious, the multipath routing algorithms take much more time than Friends scheme which detects the malicious activity by checking the challenge reply. This on the other hand reduces overheads and hence reduces the chances of unsecured routing through faulty nodes. In the future, we plan to implement existing secure routing protocols such as the ARIADNE and ARAN and compare them with the proposed Data Encryption Friend Based Routing Protocol. This would give a better picture about the standing performance of the security based algorithm for MANETs.

REFERENCES

[1] W. Diffie and M. E. Hellman, “New directions in cryptography,” IEEE Trans. Inform. Theory, vol. IT-22, no. 6, pp. 644–654, 1976.

[2] M. S. Obaidat and N. Boudriga, Security of e-Systems and Computer Networks. Cambridge, U.K.: Cambridge Univ. Press, 2007.

[3] Y. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks,"Wireless Netw., vol. 11, no. 1–2,pp. 21–38, Jan. 2005.

[4] M. G. Zapata and N. Asokan, "Securing ad hoc routing protocols," in WiSe'02: Proc. of 1st ACM Workshop on Wireless Security, Atlanta,GA, Sep. 28, 2002, pp. 1–10.

[5] P. Papadimitratos and Z. J. Haas, "Secure link state routing for mobile ad hoc networks," in IEEE International Symposium on Applications and the Internet-Workshop on Security and Assurance in Ad Hoc Networks, Orlando, FL, Jan. 2003, p. 379.

AUTHORS PROFILE

Ms SHARMILA.G, Presently Pursuing Final Year M.TECH CSE, In PRIST University, Puducherry Campus, Puducherry, India

Ms.J.R.Thresphine, Received The M.Tech In Computer Science And Engineering. Presently she is a Working Assistant Professor in Computer Science and Engineering at PRIST University, Puducherry Campus, and Puducherry, India.

