Manet Adaptive Routing To Enhance Security Using Artificial Immune System

V.Vinodhini[*], R.Shivadharshini[*], S.Sangeethapriya[*], P.Kanagaraju**

[* Final Year B.E (CSE), K.S. Rangasamy College of Technology, Tiruchengode]
[** Assistant Professor, K.S. Rangasamy College of Technology, Tiruchengode]

E-mail id: shivacse10@gmail.com,mailofvinovisha@gmail.com

Abstract— Wireless devices and the increase of computing and storage resources are increasing in supporting mobile computing environments. Especially, ad hoc networks can probably connect different wireless devices. The infrastructure less and the dynamic nature of Mobile Ad hoc Network (MANET) demands new set of networking strategies to be implemented in order to provide efficient end-to-end communication. The entire network is mobile and the individual terminals are allowed to move freely. The nodes can be located anywhere such as in or on airplanes, ships, trucks, cars, even on people or very small devices. Routing is a big problem in Mobile ad hoc networks. Different types of protocols had been proposed so as to increase efficiency and security of data transmission in Mobile ad-hoc networks (MANET), but they are indicated as a matter of concern for computation overhead which leads to impracticability. Though adaptive routing minimizes the problem of efficiency, it doesn't cover the secure issues. A possible reason for node misbehavior is faulty hardware or software. Another reason is that to save its battery power. In such a condition, battery replacement may not be possible. Each node depends on small low-capacity batteries as energy sources and cannot expect replacement when operating in hostile and remote regions. Centralized and distributed scheduling algorithms. This could bring in a considerably throughput improvement with the variation of node density such as link failure ratio, packet arrival rate, retransmission threshold. To enhance efficiency and security for misbehaving node detection integrate security mechanism based on Artificial Immune System (AIS) with adaptive routing strategy. In initial phase, the detection systems listens to the normal behavior of the nodes by means of the DSR protocol and in second phase detection and classification are performed to prevent unauthorized access to the data packets.

Keywords— Adaptive Routing, Attacks, Artificial Immune System (AIS), High throughput, Mobile Ad Hoc Networks (MANET), Node misbehavior, Security, etc.

I. INTRODUCTION

A. Mobile Ad Hoc Networks

A mobile ad hoc network (MANET) is a network consisting of a collection of nodes capable of communicating with each other without the help from a network infrastructure. Nodes that lie within all other mobile node's send range can communicate directly and they are responsible for dynamically discovering the other nodes within their radio ranges. For communication between nodes that are not directly within established node's send range, intermediate nodes act as routers that relay packets generated by other nodes to their destination. These nodes are often energy constrained devices with a great diversity in their capabilities. Moreover, devices have the ability to freely join or leave the network and make movements randomly, thus potentially resulting in rapid and unavoidable topology changes. In addition, these networks are facing the traditional problems intrinsic to the wireless communications such as lower reliability than wired media, less physical security, battery restrictions, time varying channels, obstruction to the data transmission, etc.

B. Routing In Mobile Ad Hoc Networks

The extremely dynamic nature of a mobile ad hoc network results in frequent and irregular changes of network topology further concerns the routing among the connected nodes. The complications and added with the significance of routing protocol in establishing communications among mobile nodes, make routing area the most vigorous research area within the MANET. Various routing protocols and algorithms had proposed earlier in various researches, and their performance had been comparatively studied under different network situations and traffic conditions.

MANET is distinguished from the traditional kinds of network by establishing a more dynamic environment, continuously changing network topology due to mobility of nodes to be organized together. The feature makes it difficult to perform routing in a MANET compared with a conventional wired network. The more prominent and efficient routing protocols had been proposed. These protocols can be seen in the following basic three categories:

a) Reactive routing protocols

b) Proactive routing protocols

c) Hybrid routing protocols

On-demand protocols meet with a lower network load on comparison with the table driven protocols as the nodes need not make constant update of the routing tables. But, the route acquisition delay is increased as the routing messages have to be communicated every time before message passing is possible over a new route. Major MANET routing protocols, based on reactive routing schemes, are Ad hoc On-demand Distance Vector (AODV) and Dynamic Source Routing (DSR), have been used.

Typical table driven protocols are highly dynamic Destination-Sequenced Distance Vector Routing (DSDV) and Optimized Link State Routing (OLSR).Table driven routing protocols have a low route acquisition delay because each node always has to maintain a fresh route to all other nodes of network. Though, the storage, bandwidth, and power requirements are high since each node must keep its routing table up-to date which mandates periodic routing message exchanges.

Hybrid protocols have a lower route acquisition delay than the reactive counterparts and a lower overhead than proactive routing schemes. These protocols, although, are not suitable for highly dynamic MANET environments as it is simply infeasible to delegate roles to nodes and divide the network into zones under such network conditions.

C. Security Attacks against Routing In Manets

Routing is one of the most important services in the network. Moreover it is also one of the major concerns as it is being targeted by the attackers who aim to conduct their malicious behaviors. Although security issues in MANET is vitally focused in the current years, the development of completely secured schemes and mechanisms for such network has not been successfully achieved till now.

The attacks related to MANET security routing can be classified as the following major types,

1. Passive attacks
2. Active attacks.

The motive of a passive attack is to listen and retrieve important information residing inside the data packets, as an instance of discharging a traffic monitoring attack. In this attack, a malicious node makes a try to identify and locate communication parties and functionality which provide a message to launch supplementary attacks. This attack type is called passive since the normal functionality of the network is not changed. An active attack is done by a malicious node with the intention to interrupt the routing functionality of the entire network.

1) Malicious Nodes

These nodes can disrupt proper functioning of routing protocols by changing routing information. These nodes may falsify the routing information and pretend to be other nodes. On the other hand selfish nodes by simply refusing to participate can be reduced the operation of the network performance. The premium types of active attacks are making a tunnel in the network between malicious node that is via it to make a private connection and circumvention network. This kind of attack makes the normal flow of routing messages to be short circuited by a node constructing a virtual vertex cut in the network. In order to destabilize the network traffic, false nodes carried out attacks that can easily be integrated by the modification of routing protocols by the malicious nodes.

II. EXISTING SYSTEM

A. Adaptive Routing

In adaptive routing, devices have to make a decision on the usage of appropriate and optimal routing technique depending on the ad hoc network type they participate in and the current network conditions such as traffic load, network bandwidth, etc in the network. The multiple compatible modes of operation have been approached in the adaptive multi-mode routing protocol, where each mode is designed to operate as efficiently as possible to make an efficient transmission. Simulation studies, analytical studies, and

models are used to find out the optimal network conditions of the various defined modes. The vast problem in the development of such a framework is that nodes need to be capable of monitoring and estimating the network conditions in their environment with as much little overhead as possible. The predictions nodes can alter their mode of operation based on that estimation to the networking context and perform the best possible routing. Adaptive routing is designed to perform better without disrupting service or the degradation of performance.

When mobile nodes are active in the network, they can make new links with the already existing nodes or may break the link with the other nodes with similar or different modes that demands various actions of the adaptive routing protocol. Due to the nodes' mobility the routing control overhead is increased resulting in more amount of proactive-ness in the network also the number of routing control packets needed increased simultaneously. These nodes can make a selection of the mode individually and randomly and protocol correctness has also been offered in mobile networks.

Different MAC schemes have been designed to exploit the inherent features to improve the throughput and reliability. The design of MAC scheme in multi-hop network is very difficult.

B. Modes in Adaptive Routing

The following three modes have been developed:

1) Mode 1

Nodes in MODE 1 need not proactively announce their location by propagating distance vectors to all other nodes. If any other node wants to communicate with that node, it has to establish a route that is reactive to the network. It is necessary that all nodes must support MODE 1.

2) Mode 2

A set of consistent nodes in MODE 2 must keep an up-to-date route to every other node via the propagation of distance vectors. The propagation is limited to nodes that are in MODE 2 or MODE 3 and provide support for MODE 2. When a node in MODE 1 receives such an update it will not broadcast it rather discards it. The mode usually creates clusters of nodes that proactively maintain routes to each other.

3) Mode 3

Unlike MODE1 and MODE2, nodes in MODE 3 make a proactive announcement of their location through the propagation of distance vectors. It provides support for additional propagation of the information.

C. Disadvantages of Existing System

- Less throughput
- Poor reliability
- Path loss
- Topology & link breakages
- Misbehaving nodes in the MANETs can disrupts the messages passed between the nodes
- It is limited to medium and large time-scale network changes when adapting
- Packet delivery ratio drops and also the traffic load increased as mode switch frequency increases

III. PROPOSED SYSTEM

The adaptive routing takes place between the nodes using the adaptive algorithm, termite. In our proposed system, we are implementing the Artificial Immune System (AIS) to prevent the unauthorized access to the data transmitted. These systems are inspired by the Biological Immune System (BIS). In this approach, the misbehaving nodes are detected using the negative selection algorithm. In an initial phase, the detection system is intended to identify the normal behavior in accordance with the DSR protocol. After that they enter the second phase where detection and classification are done. If there are relatively many suspicious intervals for a neighbor, that neighbor is classified as misbehaving.

The immune system is highly distributed, highly adaptive; self-organizing in nature. This system maintains a memory of past encounters and continues to learn about new encounters. AIS systems are developed around the recent understanding of the immune system. AIS can be implemented easily when compared to the genetic algorithms. Security always indicates the identification of possible attacks, vulnerabilities and threats of a certain system.

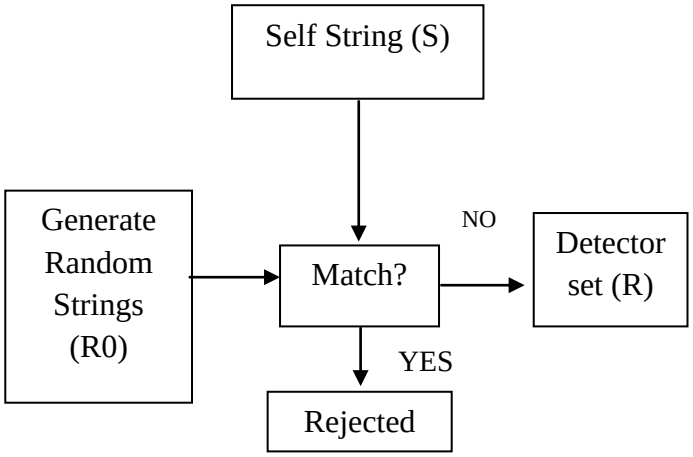

Fig. 1 Negative Selection Algorithm

The proposed system is described as follows that provide the various features such as

- To mathematically model the problem and provide a centralized algorithm
- To provide simple as well as effective distributed scheduling algorithms through the two phases of the problem
- To detect misbehaving nodes using negative selection algorithm
- Artificial Immune System (AIS) to prevent the unauthorized access to the data transmitted
- Misbehaving nodes are detected using the negative selection algorithm
- To propose a simple relay scheme to formulate relay set and invoke relay transmission without extra signaling overhead

MANET security in artificial immune system is suitable for use in MANET routing security. Decentralization and stability in the MANET nodes are the key characteristics. Same variable system that can be defined by a centralized system would get affected. Different kinds of artificial immune system have been developed for a wide range of applications including fraud detection and host-based intrusion detection. To make protection to the nodes, immune agent is formed by using artificial immune system. The immune agents existing in the basic nodes in domain and a copy of this artificial immune to networked mobile node inputs have to be sent during new set up of connection.

A. Modules in the Proposed System

The proposed model consists of the following modules such as,

- Adaptive relay
- Relay transmission by scheduling data packets
- Relay operations
- Artificial Immune System(AIS)

1) Adaptive Relay

The main purpose of this module is to exploit the diversity concurrently and multiplexing for transmission robustness and higher throughput. The advantage of using this module is obtaining the relay packets without any extra overhead. This module is responsible for the detection of new links and link breaks and for relaying information to the routing protocol about the existing links. This information gets stored in a neighbor table that can be consulted by the routing protocol and monitoring agent. The detection of created links and breakages of link can occur through the exchange of beacon messages.

The primary usage of this module can be described as follows,

- Forwarding of relay packet as well as normal packet transmissions
- Transmitting the data packet through intermediate nodes using the established cost value paths
- Synchronization requirements coupled with the multi-stream reception capability of receivers

2) Relay Transmission By Scheduling Data Packets

In this module of packet scheduling, a simple formulation of a candidate relay is set for a packet. The network is a random mixture of proactive and reactive routing and the protocol is able to correctly deliver most packets to the destination and to achieve a

better performance. To make an efficient transmission, a simple priority-based relay selection without extra signaling takes place on the mobile nodes.

Its advantage is,

- Support load balancing and reduce delay impact on candidate nodes
- Reduce redundant relay transmission in the Receiver-enhanced nodes

3) Relay Operations

For the adaptive multi-mode routing protocol, both reactive and proactive mode can be implemented. The nodes using proactive modes maintain distance vectors to route the basic information for its functioning. This proactive mode can be refined further based on the number of destinations for which the routing table data is propagated proactively from a single destination to many destinations in the network and the life of propagation from neighbors to the entire network. The frequency of the intermittent distance vector exchange can differ depending on the measured mobility of the nodes. Every node chooses its optimal mode based on the mobility and the moment the node changing its location. It determines how the node can propagate its information within the network and how well the node interactions take place. So, a node can have routing table entries for different modes in its routing table.

The primary function for the module of relay operations can be described as follows,

- Finding Candidate Relay Nodes
- Triggering of Relay Transmission
- Limit the Delay of Transmission

4) Artificial Immune System (AIS)

The nodes in an ad hoc network also function as routers that discover and maintain routes to other nodes in the network. The primary goal of a MANET routing protocol is to establish a correct and efficient route between a pair of nodes so that messages may be delivered in a timely manner. If routing can be misdirected, the entire network can be stopped from functioning. Thus, routing security plays an important role in the security of the whole network.

Since mobile nodes involve in the communication, the reason of node misbehavior can be found to be a faulty hardware or software

- Integrate the security mechanism based on Artificial Immune System
- To determine the network unsafe nodes
- To improve the efficiency of the packet exchange
- To provide security for misbehaving node detection
- To remove network unreliable nodes
- Detect holes in the routing path Using the negative selection algorithm

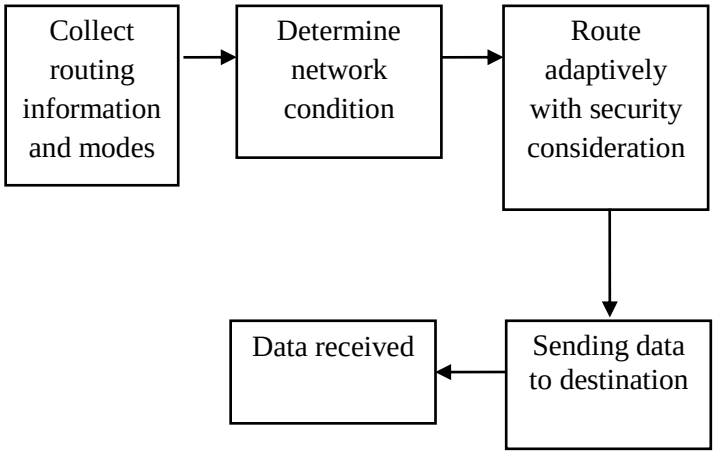

Fig. 2 Secure adaptive routing

B. Advantages of Proposed System

- Multiplexing
- High Throughput and reliability
- Fast Transmission and optimal route paths
- Secure
- Packet delivery ratio can be maximized
- Less load on the network traffic

IV. CONCLUSION

MANET is an emerging research area with practical applications. But, a wireless MANET indulges a greater security problem than its conventional wired and wireless counterparts due to its fundamental features of open standard, dynamic topology, and absence of central authorities, distributed co-operation, and constrained capability. Routing security plays an important role in the security of the entire network.

Adaptive routing is used to overcome the control overheads met in proactive protocols and the network loads in reactive protocols together, by the periodic exchange of hello messages. The biggest challenge is the mapping of the different routing protocol modes to the observed network context. Also, the secure transmission can be implemented using the Artificial Immune System (AIS) which detects the misbehaving nodes in the network and avoids data transmission through those nodes. Here usage of the negative selection algorithm detects the holes in the routing path and report it to the protocol to prevent the loss of transmission.To achieve security in MANETs, routing protocol is important work that the unique characteristic of Ad hoc wireless networks a challenging. In the recent years the use of the natural human immune system in computing systems leads to the implementation of artificial immune system in networks by the different applications. The wide usage of these systems is designed based on the model of insiders and outsiders. The vital study about the application of danger theory presents the artificial immune system to be used in the detection and prevention of attacks in MANET can be very beneficial. In this paper an overview of the different security indications, related security threats and detection of misbehaviour nodes on DSR routing protocol could be determined.

REFERENCE

[1] Abhay Kumar Rai, Rajiv Ranjan Tewari and Saurabh Kant Upadhyay (2010), "Different Types of Attacks on Integrated Manet-Internet Communication", International Journal of Computer Science and Security, Vol. 4, No. 3, pp. 265-274.

[2] Behzad Mahdavi1, Bahram Najafpour and Saeid Nejhad Hoseini (2013), "Application of Artificial Immune System for Detection of Misbehaviour Nodes in Mobile Ad Hoc Network", Journal of Basic and Applied Scientific Research, Vol. 3, No. 1, pp. 160-164.

[3] Cong Liu and Jie Wu (2008), "Adaptive Routing in Dynamic Ad Hoc Networks", IEEE Wireless Communications and Networking Conference, pp. 2603-2608.

[4] Hu Yiqing, Xiong Yan and Lu Qiwei (2013), "A Secure Adaptive Routing Strategy Using Immune Mechanism in MANET", Chinese Journal of Electronics, Vol. 22, No. 4, pp. 784-788.

[5] Jeroen Hoebeke, Ingrid Meorman, Piet Demeester (2012), "Adaptive Routing for mobile ad hoc networks",

[6] Mamatha T. (2012), "Network Security for MANETS", International Journal of Soft Computing and Engineering, Vol. 2, No. 2, pp. 65-68.

[7] Neha Kaushik and Ajay Dureja (2013), "Performance evaluation of modified AODV against black hole attack in manet", European Scientific Journal, Vol. 9, No. 18, pp. 182-193.

[8] Qingting Wei and Hongzou (2008), "Efficiency Evaluation and Comparison of Routing Protocols in MANETs", International Symposium on Information Science & Engineering, Vol. 2, pp. 175-177.

[9] Seon Yeong Han and Dongman Lee (2013) ,"An Adaptive Hello Messaging Scheme For Neighbour Discovery In On-Demand Manet Routing Protocols", IEEE Communication Letters, Vol. 17, No. 5, pp. 1040-1043.

[10] Xiaoxin Wu and Bharat Bhargava (2005), "AO2P: Ad-Hoc On Demand Position-Based Private Routing Protocol", IEEE Transactions on Mobile Computing, Vol.4, No. 4, pp. 335-348