ENSURE DATA TRANSMISSION IN MOBILE AD-HOC NETWORKS

M. Kavitha
P.G. Scholar, Dept. of CSE
A.S.L. Pauls CET
Solavampalayam, Coimbatore
mkavitha_be@yahoo.co.in

T. Maheshwaran
Asst. Prof., Dept. of CSE
A.S.L. Pauls CET
Solavampalayam, Coimbatore
waranmahesh20@gmail.com

Prof. M. Senthil Kumar
Associate Prof. & Head
Ranganathan Engg. College
REC Kalvi Nagar, Coimbatore
kathir_senthil@yahoo.co.in

Abstract: In the existing faith management scheme, the faith model has two components: faith from direct observance and faith from indirect observance. With direct observation from an observer node, the trust value is derived using Bayesian inference, which is a type of unsure conclusion when the full probability model can be defined. On the other hand, with indirect observance, also called secondhand information that is obtained from neighbor nodes of the observer node, the trust value is derived using the Dempster-Shafer concept, which is another type of uncertain reasoning when the proposition of interest can be derived by an indirect method. We proposed DES concept to encrypt the data between source and destination. In this method used for securely transmit the data and achieve the secure data transmission in mobile ad hoc network.

Keywords: MANETs, DES, Alert-based Approach.

1. INTRODUCTION

With recent advances in wireless technologies and mobile devices, Mobile Ad hoc Networks (MANETs) become popular as a key communication technology in military tactical environments such as establishment of communication networks used to coordinate military deployment among the soldiers, vehicles, and operational command centers. There are many risks in military environments needed to be considered seriously due to the distinctive features of MANETs, including open wireless communication medium, nomadic and disseminated nature, and lack of centralized infrastructure of security protection. Therefore, security in tactical MANETs is a challenging research topic.

(Fig. 1) Mobile Ad-Hoc Network

There are two complementary classes of approaches that can safeguard tactical MANETs: Alert-based and catching based approaches. Alert-based approaches are studied comprehensively in MANETs. One issue of these Alert-based approaches is that a centralized key management structure is needed, which may not be realistic in distributed networks such as MANETs. In addition, a centralized infrastructure will be the main target of rivals in fields. If the infrastructure is destructed, then the whole network may be paralyzed. Furthermore, although alert-based approaches can prevent misdeed, there are still chances remained for malicious nodes to participate in the routing procedure and disturb proper routing establishment. From the experience in the design of security in cabled networks, multi-level security processes are needed. In MANETs, this is especially true given the low physical security of mobile devices. Serving as the second wall of protection, detection-based approaches can effectively help identify malicious activities.
2. RELATED WORKS

Trust-based security schemes are important detection-based methods in MANETs, which have been studied recently. In the trust value of a node based on direct observation is derived using Bayesian methodology. The authors of regard trust as uncertainty that the observed node performs a task correctly, and entropy is used to formulate a trust model and evaluate trust values by direct observance. Compared to direct observance in trust evaluation, indirect observance or second-hand information can be important to assess the trust of observed nodes. For example, the collection of testimonies from neighbor nodes can detect the situation where a hostile node performs well to one observer, while performing poorly according to another node.

Trust based security systems are also studied in different network architectures, e.g., wireless sensor networks, vehicular ad hoc networks (VANETs), cooperative wireless networks, etc. Although different types of networks have different specific characteristics, the proposed trust model based on direct and indirect observation is general enough and can be customized to a particular network.

To make it easier to understand the proposed trust model, we present an overview of OLSRv2 and the vulnerabilities of OLSRv2. OLSRv2 is a proactive routing protocol, which is a new version of OLSR. OLSRv2 inherits OLSR’s core algorithms and also introduces some new features: routing Multipoint Relay (MPR), flexible link metrics, extensible content formats, etc. OLSRv2 has three basic components: Neighborhood Discovery, MPR Selection, and Topology Establishment, as well as two types of control messages: a HELLO message and Topology Control message. Neighborhood Discovery is used to facilitate a node’s discovery of its one-hop neighbors in radio range.HELLO messages, which can carry link status such as symmetric, asymmetric, or multipoint relay, are used in the neighborhood discovery procedure. Through periodically sending HELLO messages, a node can establish bi-directional (symmetric) links with its one-hop neighbors. Two types of MPR selection: flooding MPR selection and routing MPR selection are performed in OLSRv2. Flooding MPR selection plays a key role in forwarding control traffic in the network. A node selected by a neighbor of this node as a flooding MPR will forward the message from the neighbor once.

3. EXISTING SYSTEM

A unified trust management scheme that enhances the security in MANETs using unsure conclusion. In the proposed scheme, the trust model has two components: trust from direct observance and trust from indirect observance. With direct observance from an observer node, the trust value is derived using Bayesian inference, which is a type of unsure conclusion when the full probability model can be defined. On the other hand, with indirect observation from neighbor nodes of the observer node, the trust value is derived using the Dempster-Shafer concept, which is another type of uncertain reasoning when the proposition of interest can be derived by an indirect method.

3.1 Issues

In existing system, when comparing direct and indirect observation values to confirm the original node and attacker node in network, there are chances for classified attacker node as original node in network is based on false report with direct and indirect observation.

4. PROPOSED SYSTEM

DES method is proposed to encrypt and send data between source and destination in network. In this system, user is given to send the data from source to destination and that data has to be converted into encrypted format using DES method. This process is
used for achieving the secure data transmission in mobile ad hoc network.

In this module used to provide the security for data’s in the network through DES to encrypt the data and send source to destination in network. DES concept used to encrypt the data between source and destination in the network. Through this process secure data transmission in mobile ad hoc network.

(Fig. 2) Encryption

(Fig. 3) Secure Data Transmission

4.1 Node Generation and Configuration

The needed number of nodes is generated by using the node command in NS2. The nodes are disseminating in a wireless environment. The random motion is set as true. So, the nodes are moving in a random direction. Each node is considered as an autonomous node. The nodes are configured as to process in MANET environment. The node configuration is done by using node-config command. We have to specify the Channel used by the node, Radio propagation model, Link layer type, Physical layer type, Type of interface queue and the protocol used to route the packets dynamically.

(Fig. 2) Encryption

4.2 Route Generation

In route generation module we are routing the route between source and destination in network, to find out the neighbor nodes between source and destination and find the link quality of each every node in route between source and destination. To verify the node link quality, the appropriate route to be chosen between source and destination.

(Fig. 3) Secure Data Transmission

4.3 Encryption

5. EXPERIMENTAL RESULTS

During simulation time the events are traced by using the trace files. The function of the network is evaluated by executing the trace files. The events are stored into trace files while executing stored procedure. In this procedure, we trace the events like data received, data lost, Last data received time etc. These trace values are write into the trace files. This procedure is continually called for every 0.05 ms. so, trace values stored for every 0.05 ms.

Figure 4 shows network throughput to be increased by using this secure data transmission in mobile ad-hoc network.

Figure 5 shows packet loss ratio to be decreased in secure data transmission in mobile ad hoc network.
6. CONCLUSION

In this paper, we have proposed DES method for secure data transmission in mobile ad hoc network and using this method we can increase the network throughput and also decrease the packet loss ratio among in the network. In this process we use DES scheme for encrypted the data between source and destination. This process can achieve the secure data transmission in mobile ad hoc network.

REFERENCES


