World Applied Sciences Journal 29 (Computer Sciences, Engineering and Its Applications): 126-130, 2014
ISSN 1818-4952

DOI: 10.5829/idosi.wasj.2014.29.csea.2241

An Anomaly Detection Scheme in Mobile AD HOC Network

K.P. Thooyamani, R. Udayakumar and V. Khanaa

School of Computing Science, Bharath University, Chennai-73, India

Abstract: Mobile Ad hoc network (MANET) is a kind of wireless network which has no infrastructure. Security is an essential requirement in mobile ad hoc network to provide protected communication between mobile nodes. Due to unique characteristic of MANETs, it creates a number of consequential challenges to its security design. In this paper, we propose a new anomaly-detection scheme for Dynamic MANET On-demand (DYMO) Routing protocol based on dynamic learning process that allows IDS system to monitor the network and updating the training data at particular time interval. In the dynamic environment, a trustable node (IDS system) in the network will do monitor process of each node in the network using dynamic training data. The dynamic learning process involves calculating the projection distances based on multidimensional statistics using weighted coefficients. For maintaining security the data packet are send in the encrypted format using RSA algorithm.

Key words: Projection distances · Multidimensional statistics · Weighted coefficients · DYMO protocol

INTRODUCTION

In general, mobile ad hoc networks are formed dynamically by an autonomous system of mobile nodes that are connected via wireless links without using the existing network infrastructure or centralized administration. The nodes are free to move randomly and organize themselves arbitrarily; thus, the network wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. Mobile ad hoc networks are infrastructure-less networks since they do not require any fixed infrastructure, such as a base station, for their operation. In general, routes between nodes in an ad hoc network may include multiple hops and hence it is appropriate to call such networks as ‘‘multi-hop wireless ad hoc networks’’. Each node will be able to communicate directly with any other node that resides within its transmission range. For communicating with nodes that reside beyond this range, the node needs to use intermediate nodes to relay the messages hop by hop. The ad hoc networks flexibility and convenience do come at a price. Ad hoc wireless networks inherit the traditional problems of wireless communications and wireless networking.

- The wireless medium has neither absolute, nor readily observable boundaries outside of which stations are known to be unable to receive network frames.
- The channel is unprotected from outside signals;
- The wireless medium is significantly less reliable than wired media.
- The channel has time-varying and asymmetric propagation properties.
- Hidden-terminal and exposed-terminal phenomena may occur.

To these problems and complexities, the multi-hop nature and the lack of fixed infrastructure add a number of characteristics, complexities and design constraints that are specific to ad hoc networking.

MANETs Salient Characteristics

Dynamic Topologies: Nodes are free to move arbitrarily; thus, the network topology which is typically multihop- may change randomly and rapidly at unpredictable times and may consist of both bidirectional and unidirectional links.

Corresponding Author: R. Udayakumar, School of Computing Science, Bharath University, Chennai-73, India.

Bandwidth-constrained, Variable Capacity Links: Wireless links will continue to have significantly lower capacity than their hardwired counterparts. In addition, the realized throughput of wireless communications-after accounting for the effects of multiple access, fading, noise and interference conditions etc. is often much less than a radio's maximum transmission rate. One effect of the relatively low to moderate link capacities is that congestion is typically the norm rather than the exception, i.e. aggregate application demand will likely approach or exceed network capacity frequently. As the mobile network is often simply an extension of the fixed network infrastructure, mobile ad hoc users will demand similar services. These demands will continue to increase as multimedia computing and collaborative networking applications rise.

Energy-constrained Operation: Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design criteria for optimization may be energy conservation.

Limited Physical Security: Mobile wireless networks are generally more prone to physical security threats than are fixed-cable nets. The increased possibility of eavesdropping, spoofing and denial-of-service attacks should be carefully considered. Existing link security techniques are often applied within wireless networks to reduce security threats. As a benefit, the decentralized nature of network control in MANETs provides additional robustness against the single points of failure of more centralized approaches.

Security Issues: The network topology of MANETs frequently changes and there is no central management entity, all of the routing operations must be performed by the individual nodes in a collaborative fashion. Consequently, it is unrealistic to introduce an authentication server that can employ conventional cryptographic schemes to secure the network against attacks from malicious hosts. The typical types of attacks in MANETs include eavesdropping, address spoofing, forged packets, denial of service (DoS), etc.

Secure routing protocols in which key-based cryptographic technologies are applied have been suggested to meet the increasing demands for MANET security. However, besides the topology issue, these methods cannot protect the network from attacks by a malicious node that has managed to acquire the network key. Therefore, other security methods that can detect attacks from malicious hosts are required.

The techniques for detecting the malicious attacks are usually classified into two categories, namely, misuse detection and anomaly detection. In misuse detection, the method of using a signature-based analysis is widely implemented. In this method, the attacks are identified by comparing the input traffic signature with the signatures extracted from the known attacks at the network routers. Anomaly detection is a technique that quantitatively defines the baseline profile of a normal system activity, where any deviation from the baseline is treated as a possible system anomaly. It is rather easy to detect an attack, the traffic signature of which is identifiable by using misuse detection. However, for those attacks, the type or traffic signatures of which are hard to identify by misuse detection, the method is rather inadequate. In such cases, those attacks can only be detected by using anomaly detection methods. In anomaly detection, even when the traffic signature is unknown, if the baseline profile of a network is delineated *a priori*, then the abnormality can be recognized.

In the effectiveness of such detection method in wired networks has been demonstrated. In this method, the baseline profile is preextracted and then applied to the same network. However, for MANETs, since the network conditions are likely to change, the preextracted network state may not correctly represent the state of the current network. This problem indeed influences the accuracy of the anomaly detection method. Due to the fact that the MANET environment dynamically keeps evolving, envisioning a robust anomaly detection method becomes imperative to thwart the malicious attacks against it. In this paper, we propose a new anomaly-detection scheme for Dynamic MANET On-demand (DYMO) Routing protocol based on dynamic learning process that allows IDS system to monitor the network and updating the training data at particular time interval. In the dynamic environment, a trustable node (IDS system) in the network will do monitor process of each node in the network using dynamic training data. The dynamic learning process involves calculating the projection distances based on multidimensional statistics using weighted coefficients. For maintaining security the data packet are send in the encrypted format using RSA algorithm.

Related Work

Secure Schemes for Routing Procedures: Secure ad hoc routing protocols have been proposed as a technique to enhance the security in MANETs. For example, the secure AODV (SAODV) [1], which uses signed routing messages, is proposed to add security to AODV [2]. Zhou and Haas proposed a distributed certification authority mechanism in which the authentication uses threshold cryptography [3]. A MANET is divided into clusters and a certification authority is appointed to each cluster. These methods can only guard against external attacks. However, the internal attacks mounted by the malicious or compromised hosts may still have a severe impact on the network performance, as well as on the connectivity among the nodes in the targeted MANET. A previous method requires the intermediate node to send the route confirmation request (CREQ) [4] to the next hop node toward the destination and then, the next hop node receives the CREQ and looks into its cache for a route to the destination. If it has such a route to the destination, then it sends a route confirmation reply (CREP) message to the source node with its route information. The source judges whether the path in RREP is valid by comparing the information with CREP. In these methods, the routing protocol has to be modified. These modifications may increase the routing overheads, which results in the performance degradation of the bandwidth-limited MANETs.

Network Monitoring-Based Attack Detection: The techniques of attack detection by network monitoring, which can detect attacks from inside MANETs, have also been proposed. For instance, Kachirski and Guha [5] proposed a method that detects attacks by employing distributed mobile agents. Network monitoring nodes are selected to be able to collect all the packets within a cluster and the decision agents in the nodes are used to detect and classify the security violations. The concern of this method is that the monitoring nodes will consume a large amount of energy. Vigna *et al*. [6] detect attacks by placing AODV-based State Transition Analysis Technique (AODVSTAT) sensors within the network and by either observing solely contiguous nodes or trading information with other sensors. However, it is necessary to deploy a large number of AODVSTAT sensors on the nodes for detecting a varied range of attacks. In addition, a large number of UPDATE messages may cause an overwhelming congestion in the network.

Anomaly Detection: Huang *et al*. [7] constructed an extended finite-state automaton (EFSA) according to the specification of the AODV routing protocol, envisioned normal condition modeling and detected attacks with both specification-based and anomaly-based detection schemes. In specification-based detection, the attacks were detected as deviant packets from the conditions defined by EFSA. In addition, in anomaly detection, the normal conditions are defined as the baseline with which the condition of EFSA and also the amounts of transition statistics are compared. The deviations from those conditions are then used to detect the potential attacks. For determining the baseline profiles, in both methods, the training data are extracted beforehand from the same network environment where the test data are applied. However, we note that the MANET topology can rather easily be changed and the differences in network states grow larger with time. Furthermore, these methods cannot be applied to a network where the learning phase has been conducted in another network.

Proposed Work

Dynamic Learning Method to Detect Black Hole Attack: The network topology easily changes in MANET, the current state may not appropriately be expressed over time. Therefore, by only using the detection module by projection detection to define the normal state, it is rather insufficient to reflect the changing situation of MANET and a learning method that can follow these changes is indispensable. The idea of dynamically updating the training data sets is carried out by the intrusion detection system called network monitoring node. In this paper, we propose a new anomaly-detection scheme for Dynamic MANET On-demand (DYMO) Routing protocol based on dynamic learning process that allows IDS system to monitor the network and updating the training data at particular time interval.

DYMO Protocol: DYMO protocol is used for route discovery. The route discovery is used to establish routes between nodes in the network when required for communication between two nodes. A route discovery begins with an originator node multicasting a Route Request (RREQ) to all nodes in its immediate range. The RREQ has a sequence number to enable other nodes in the network to judge the freshness of the route request. The network is then flooded with RREQs until the request reaches its target node (provided that there exists a path from the originating node to the target node). The target node then replies with a Route Reply (RREP)

unicasted hop-by-hop back to the originating node. The route discovery procedure is requested by the IP network layer on a node when it receives an IP packet for transmission and does not have a route to the destination.The IP packet will then be queued in the network layer waiting for DYMO to establish the route and inform the IP layer that a route has been discovered.

The DYMO protocol has a mechanism to notify nodes about a broken route. This is done by sending a Route Error (RERR), thereby informing nodes using the route that a new route discovery is needed.

Steps to Carried out by Ids to Detect Black Hole Attack: In the dynamic environment, a trustable node (IDS system) in the network will do monitor process of each node in the network using dynamic training data by updating the training data at particular time interval.

Feature Selection: To express state of the network by IDS system, multidimensional feature vector is defined. Each dimension is counted up on every time slot. In order to detect attack, the negative acknowledgement is taken into account. In normal state due to congestion, packets are unreachable to the destination. Therefore the receiver sends NACK to the sender and also due to RERR, receiver sends NACK to the sender.

In network during abnormal state, the source always selects the highest destination sequence number. The destination response to the route request message by sending RREP with destination sequence number. Therefore the source selects the highest destination sequence number. When the source sends the packets, the packets are dropped by the malicious node. In the mean time the destination waiting to receive the packets. if the packet are unreachable to the destination it sends the NACK to the source. Even the NACK is dropped by the malicious node, but through alternative path NACK reaches the source. All these process are monitored by the network monitor node and side by side updates the training data by considering only the normal state.

Detection Module by Projection Distance: For the traffic that flow across each node, the network state in time slot i is expressed by three-dimension vector $x_i = (x_{i1}, x_{i2}, x_{i3})$. Here, the groups of normal states are considered to be gathered close in feature space. In contrast, the abnormal state is considered to be the scattering data that deviates from the cluster of normal state. According to this, the distribution of network state is shown if Figure 9.

we calculate the Mean vector $\bar{x}^D$ from Equation (1) using training data set D of N time slots.

$$\bar{x}^D = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{1}$$

$$d(x) = \left\| x - \bar{x}^D \right\|^2 \tag{2}$$

When the distance is larger than the threshold T_h (which means it is out of range as normal traffic), it will be judged as an attack (Equation (3)). Here, the projection distance with maximum value is extracted as Th from the learning data set.

$$\begin{cases} d(x) > T_h : attack \\ d(x) \le T_h : normal \end{cases} \tag{3}$$

Let T_0 be the current time interval and let T_1 be the first time interval. By using the data collected in T_1, initially, the first principal element is calculated and then the calculated first principal element is used in the following time interval T_0 for anomaly detection. If the state in T_0 is judged as normal, then the corresponding data set will be used as the training data set. Otherwise, it will be treated as the data including attack and it will consequently be discarded. This way, we keep on learning the normal states of the network.

when updating the database, it is possible to use the most recent data set. However, since the most recent data set is easily affected by the sudden change in the network, it is necessary to take the time series model into consideration to keep the database from being too sensitive to the changes in the network topology. The forgetting curve aims at reducing the weight when the data become old and of less significance.

Isolating the Dropper: In this network monitor node (detector), isolate the node which is dropping packets continuously using ENDAIRA protocol. First the detector informs to the neighbor nodes of the intruder about the dropper and asks for witness request WREQ packet with suspicious set. Suspicious set contains the droppers ID. The receiver of WREQ checks whether it has received any packet from the dropper node specified in suspicious set. If don't have knowledge about the dropper then it does not send any reply to the detector or otherwise it sends WREP to the detector. Finally the detector broadcast an Accusation packet (PC) in the n/w. Each node receives the valid Accusation and removes the node from the network.

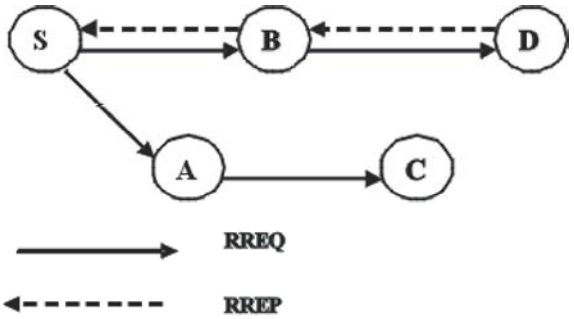

Fig 1: Route discovery using DYMO

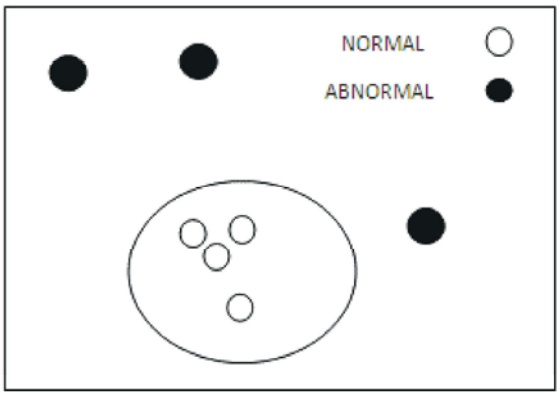

Fig 2: The distribution of network state

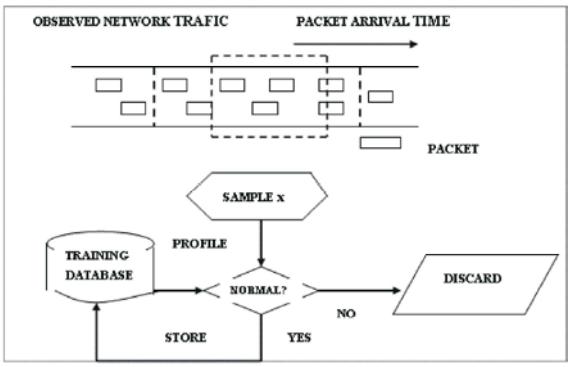

Fig 3: Flow chart learning and evaluation

CONCLUSION

In this paper, a new dynamic anomaly detection system for MANETs has been proposed. For enhancing the security in MANETs, which are vulnerable to attacks, robust learning methods against these attacks are required. To differentiate an attack state from the normal state, we have defined multidimensional features based on the characteristics of these attacks. The DYMO routing protocol provides reliable routes than AODV. The data transmission rate is increased by using DYMO protocol. The attacks are detecte The attacks are detected and protected within the time stamp limits and the malicious node is identified and isolated using ENDAIRA protocol.

REFERENCES

1. Zapata, M., 2006. Secure ad hoc on-demand distance vector (SAODV) routing, IETF Internet Draft, draft-guerrero- manetsaodv-06.txt.
2. Perkins, C., E. Belding-Royer and S. Das, 2003. Ad hoc On-Demand Distance Vector (AODV) Routing, IETF RFC 3561 (Experimental).
3. Zhou, L. and Z. Haas, 1999. “Securing ad hoc networks,” IEEE Netw., 13(6): 24-30.
4. Lee, S., B. Han and M. Shin, 2002. “Robust routing in wireless ad hoc networks,”in Proc. 31st ICPP Workshops, pp: 73-78.
5. Kachirski, O. and R. Guha, 2003. “Effective intrusion detection using multiple sensors in wireless ad hoc networks,” in Proc. 36th Annu. HICSS, pp: 57-64.
6. Vigna, G., S. Gwalani, K. Srinivasan, E. Belding-Royer and R. Kemmerer, 2004. “An intrusion detection tool for AODV-based ad hoc wireless networks,”in Proc. 20th ACSAC, pp: 16-27.
7. Huang, Y., W. Fan, W. Lee and P. Yu, 2003. “Cross-feature analysis for detecting ad-hoc routing anomalies,” in Proc. 23rd ICDCS, pp: 478-487.