Research Journal of Applied Sciences, Engineering and Technology 9(4): 277-281, 2015
DOI:10.19026/rjaset.9.1405
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: August 01, 2014 Accepted: September 13, 2014 Published: February 05, 2015

Research Article

Repeated Node Taxonomy Method for Intrusion Detection in Mobile Ad Hoc Network

[1]R. Saravanan and [2]E. Ilavarasan
[1]Department of Computer Science and Engineering, Manomaniam Sundaranar University and Saveetha Engineering College, Tamil Nadu,
[2]Department of Computer Science and Engineering, Pondicherry Engineering College, Puducherry, India

Abstract: The vital aim of the proposed node taxonomy method in Mobile Ad hoc Network (MANET) is to prevent the normal or good nodes present in the network from some infected nodes. The tainted individual nodes present in the network may affect the normal unaffected nodes in the network. To overcome that, this study proposes a novel node taxonomy method which uses the adjacency matrix. The entries in the adjacency matrix are the link strength between the nodes. The concept behind the proposed method, the node which is connected with super threshold number of known adversaries is classified as adversary. As the link between the mobile nodes changes dynamically, the node taxonomy algorithm should be executed recursively to filter out the malicious node in the network. The proposed taxonomy method has low computational cost and consumes less energy for detecting the malicious node. The proposed method is evaluated by using the Network Simulator (NS2).

Keywords: Energy, link strength, malicious node, Mobile Ad Hoc Network (MANET), performance analysis

INTRODUCTION

The security is the crucial requirements for the operation of a Mobile Ad hoc Network. Many of the Intrusion Detection Systems are proposed to find out the anomaly node present in the mobile network. Most of the Intrusion Detection System (IDS) focus only on MAC layer traffic to find the anomaly node. In the anomaly detection system provides security for three layers such as MAC layer, routing layer, application layer proposed by Bose *et al*. (2007). The profile to detect anomaly is obtained from feature vectors of the training data set. The intruder node is effectively detected by applying. Bayesian classification algorithm, Markov chain construction algorithm and association rule mining algorithm in the training data sets. If the abnormal behavior is found, that particular node is detected as the malicious node. This method provides efficient solution for intrusion detection in MANET. But, sometimes the intruder node may affect the normal node in the network.

The frontline security is strengthened by using efficient intrusion detection system. A novel intrusion detection system, which uses game theoretic model to detect the malicious node in a MANET, was proposed by Paramasiva and Pitchai (2013). Two mobile nodes interact with each other based on Bayesian game concept. Each and every mobile node continuously monitors their neighbor node and stores the information about their behaviors. The game theory uses the stored results to find the abnormal behavior of the mobile node. But this method is not suitable for energy constrained network as it continuously monitors its neighbor nodes.

Power constrained mobile nodes need the IDS which consumes less amount of energy. Generally, each node should run the IDS at all times. To overcome this, Marchang and Tripathi (2007) proposed a game theory to decide the time at which the IDS should run in the node without decreasing effectiveness of intrusion detection system. The proposed system is used to define how often one must keep the IDS running under changed circumstances.

The mobile nodes can communicate directly with the nodes which are present inside its transmission range. If the intended destination is present out of transmission range, the mobile node can transmit only via some intermediate nodes or it is called as relay nodes. This kind of communication is called as co-operative communication. All the mobile nodes may not interest to accept relay requests from other nodes. The power-constrained mobile nodes never want to spend most of its energy for relaying data. This will cause the selfishness in the network. To overcome that, proposed by Srinivasan *et al*. (2003) the Generous Tit For Tat (GTFT) acceptance algorithm which is run by the node to decide whether to accept or reject the relay request.

Corresponding Author: R. Saravanan, Department of Computer Science and Engineering, Manomaniam Sundaranar University and Saveetha Engineering College, Tamil Nadu, India

MANET is an infrastructure less decentralized network and so it has to rely on the other nodes for the communication because at most cases the destination is present outside its transmission range. The nodes believe its neighbor node and relay the data through the intermediate nodes. So, the trust plays a very important role for efficient and reliable communication. The efficient intrusion detection system is designed based on the data collected by introducing Denial of Service attack in the network proposed by Shahnawaz *et al*. (2011), which reduces the False positive rate.

The Intrusion Detection System for the MANET is designed to provide security services such as confidentiality, integrity, authentication, accuracy and availability proposed by Esfandi (2010). This study uses agents and data mining techniques to eliminate the presence of intruder node present in the MANET and tries to prove the efficiency of the proposed system.

IDS detect the intruder node by analyzing the historical record of data of each node. The feature extraction is considered as very important in the data analysis process. In the authors say that, the PCA is best to analyze the features proposed by Peyman and Mehran (2011).

This study proposes a novel node taxonomy method to filter out the malicious node in the network. This method consumes less energy to detect the malicious node. The intruder node present in the network may affect the normal node in future. So this proposed method uses the adjacency matrix to detect the anomaly node. This proposed method provides the better result by minimum energy consumption with accurate result.

PROPOSED METHODS

The malicious node present in the network behaves differently from the normal nodes and also it affects the normal node's behavior also. The performance of the node present in the network is evaluated by using the parameters like throughput, latency, data loss etc. These parameter value is deviate from the normal value in the sense that node is predicted as malicious node. In this part we say that, Nodes infected at time *t* might infect other nodes in the future. The nodes in the network should be classified repeatedly to avoid the malicious node present in the transmission. So, repeated node classification method detects the malicious nodes effectively and accurately. The repeated node classification method is described below.

Repeated node classification method: The link strength of the link exists between each and every node is estimated by using the following formula:

Link strength = Packet received rate×Received signal strength (1)

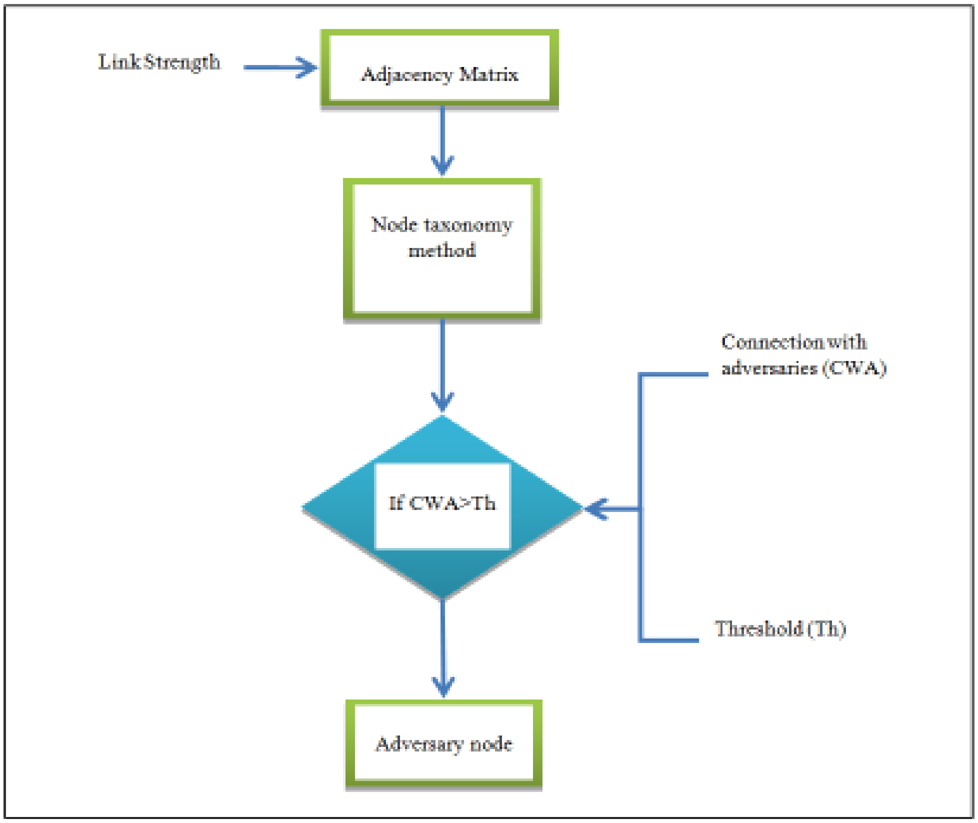

Fig. 1: Flow diagram of node taxonomy method

The link strength value is stored in the matrix M and the following steps are executed in the repeated node classification method.

Step 1: Input matrix M

Step 2: Set Si = 1 for known adversaries and to Si = 0 for the rest

Step 3: Set a threshold H

Step 4: The threshold value is calculated by using the following formula:

$$Threshold\ H = \frac{Sum\ of\ all\ entries\ in\ the\ matrix\ M}{Number\ of\ links\ exists\ between\ the\ nodes} \tag{2}$$

Step 5: For each unclassified node i, iterate from t = 1: TMAX:

$$S_i(t+1) = \Theta\left[\sum_j M_{ij} S_j(t) - H\right] \tag{3}$$

Step 6: Nodes with S (TMAX) = 1 are classified as adversaries

Procedure:

- Initially infected individuals (known adversaries)
- Nodes infected at time t might infect other nodes in the Future
- The final fraction of the infected nodes depend on the classification criterion, e.g., threshold H
- For large H only few will be infected For small enough H all nodes will be infected

As shown in Fig. 1, in the proposed method the adjacency matrix is given as input to the IDS. The adjacency matrix consists of the value of link strength. The Link Strength is defined as the duration of the link existing between two nodes. Each and every node form links with the nodes which are present inside its communication range by default. The Node Taxonomy method is clearly described by above algorithm clearly say that, the node is consider as adversary if and only if the node having connection with super threshold number of adversaries. By using IDS in the game theoretical approach (Marchang and Tripathi, 2007), we have classified the node as the adversary node and non-adversary node. The state variable plays an important role in the proposed method. The state variable will change dynamically according to the behavior of the node. The state variable is assigned as 1 for the known adversary node and 0 for rest of the nodes. The state variable is changed according to the number of connection exists with the adversary node. The state variable is updated by using Eq. (3). Node with state variable 0 is a normal node and the node with state variable 1 is an adversary node. The Node Taxonomy method is used to filter out the normal nodes that become the adversary node from the network.

RESULTS AND DISCUSSION

The performance of the proposed method is evaluated by using Network Simulator (NS2). The NS2 Simulator is mainly used in the research field of networks and communication. The NS2 is a discrete event time driven simulator which is used to evaluate the performance of the network. Two languages such as C++, OTCL (Object Oriented Tool Command Language) are used to design a wireless scenario in NS2. The C++ is act as back end and OTCL is used as front end. The X-graph tool is generally used to plot the graph. The parameters used in the simulation are tabulated in Table 1.

The packet received rate, packet dropped rate and energy consumption are the parameters used in the simulation to evaluate the proposed method.

Packet received rate: The packet received Rate is the ratio of the data packets delivered to the destination successfully. The packet received Rate is one of the important parameter to evaluate the quality of the network. The formula used to find the packet received Rate is in equation as follows:

$$PRR = \frac{No.of\ packets\ received}{Time} \tag{4}$$

Figure 2 gives the graph for packet received Rate. The graph shows that, the proposed IDS provides high

Table 1: Simulation parameters used for the proposed method

Parameter	Value
Channel type	Wireless channel
Radio propagation model	Two ray ground
Network interface type	Wireless Phy
MAC type	IEEE 802.11
interface queue type	PriQueue
Link layer type	LL
Antenna model	Omni antenna
Routing protocol	AODV
Simulation time	50 ms
Simulation area	1385×1000 m

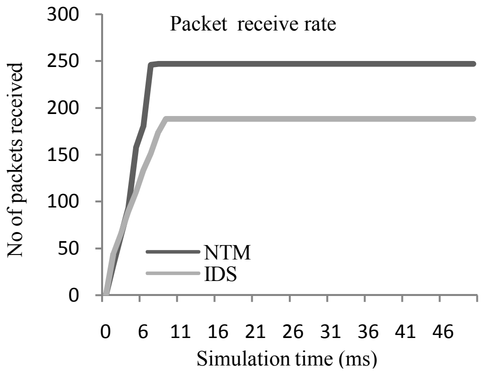

Fig. 2: Packet received rate of NTM compared with IDS

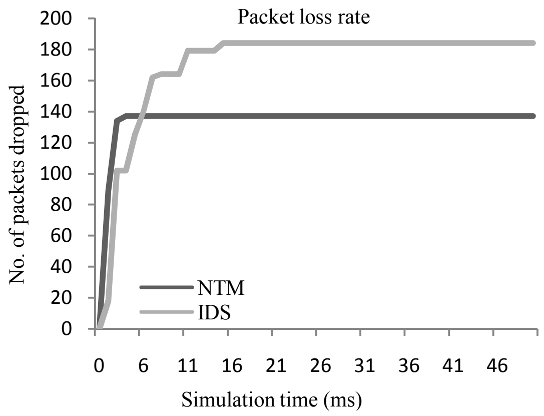

Fig. 3: Packet loss rate of NTM compared with IDs

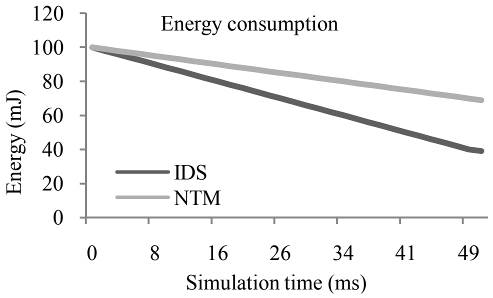

Fig. 4: Energy consumption of the node while using NTM and IDS

performance than NTM. Higher the packet received Rate indicates that the high performance of the network.

Packet dropped rate: Packet Dropped Rate is directly opposite to the Packet Received Rate. The ratio of Number of packets dropped per unit time is called as packet Dropped Rate. The Packet Dropped Rate is calculated by using the formula:

$$PLR = \frac{Number\ of\ packets\ dropped}{Time} \quad (5)$$

The packet dropped Rate is used to evaluate the quality of the network provided by the routing scheme. Figure 3 shows the graph for packet dropped Rate of the proposed scheme. Lower the packet dropped Rate indicates that the high performance of the network.

Energy consumption: The energy consumption of a node decides the life time of the node. The residual energy is calculated by using the following formula:

$$Residual\ Energy = E_T - (n * P_T)$$

where,

E_T →Total Energy
n →Number of Transmission
P_T →Transmission Power

Figure 4 shows that the proposed scheme consumes less energy because of its computational complexity. The Node taxonomy method consumes 20% of the battery power to detect the malicious node. It indicates that the proposed scheme provides the higher battery lifetime.

CONCLUSION

This study proposed a node taxonomy method to separate the malicious node present in MANET. The proposed method considers the link quality parameter to finalize the malicious behavior of the nodes. The link quality is estimated by multiplying the parameters packet received rate and the received signal strength. A malicious node does not have the highest received signal strength value because it tries to lose the packet during the transmission. The node which has the connection with the super threshold number of malicious nodes is classified as malicious node. The proposed scheme does not use any cryptography methods to strengthen the security. So, the computational cost and the energy consumption to detect the malicious node are also low for the proposed scheme. The simulation results show that the proposed scheme consumes less energy than the existing method node categorization algorithm.

Future studies can aim at using the repeated node taxonomy methods for various hybrid networks to enhance the network performance.

REFERENCES

Bose, S., Bharathimurugan, S. and A. Kannan, 2007. Multi-layer integrated anomaly intrusion detection system for mobile adhoc networks. Proceeding of the International Conference on Signal Processing, Communications and Networking, pp: 360-365.

Esfandi, A., 2010. Efficient anomaly intrusion detection system in adhoc networks by mobile agents. Proceeding of the 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), 7: 73-77.

Marchang, N. and R. Tripathi, 2007. A game theoretical approach for efficient deployment of intrusion detection system in mobile ad hoc networks. Proceeding of the International Conference on Advanced Computing and Communications. Assam, pp: 460-464.

Paramasiva, B. and K.M. Pitchai, 2013. Modeling intrusion detection in mobile ad hoc networks as a non cooperative game. Proceeding of the International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME), pp: 300-306.

Peyman, K. and A. Mehran, 2011. Feature analysis for intrusion detection in mobile ad-hoc networks. Int. J. Netw. Secur., 12(1): 42-49.

Shahnawaz, H., S.C. Gupta and C. Mukesh, 2011. Denial of service attack in AODV & friend features extraction to design detection engine for intrusion detection system in mobile adhoc network. Proceeding of the 2nd International Conference on Computer and Communication Technology (ICCCT, 2011). Allahabad, pp: 292-297.

Srinivasan, V., P. Nuggehalli, C.F. Chiasserini and R.R. Rao, 2003. Cooperation in wireless ad hoc networks. Proceeding of the IEEE Societies 22nd Annual Joint Conference of the IEEE Computer and Communications (INFOCOM), 2: 808-817.