Heterogeneous Network Based Intrusion Detection System in Mobile Ad Hoc Network

Sujithra L R[1], Nivethaa V[2], Pavithra B[3], Pavithran M[4]

[1] *Assistant Professor, Dept. of Computer Science and Engineering, Dr.N.G.P. Institute of Technology, Tamil Nadu, India*
[2,3,4] *Student, Dept. of Computer Science and Engineering, Dr.N.G.P. Institute of Technology, Tamil Nadu, India*

---***---

Abstract - *Mobile Ad hoc networks (MANET) are infrastructure-less wireless network containing self configuring mobile nodes that forms a dynamic network topology. Due to dynamic network topology, Intrusion detection systems are implemented in MANET to detect the malicious activity of mobile nodes. This in turn makes the IDS to remain active all the time that increases costly overhead for battery powered and energy consumption of nodes in the network. This paper describes the probabilistic model proposed that make use of cooperation between Intrusion Detection Systems (IDS) among neighborhood nodes to reduce their individual active time. The existing scheme is used in Homogeneous network for simulation which consists of same capacity nodes that have effective energy consumption. The proposed approach is for Heterogeneous network that have low data speed and high transmit power. Hence, we use the approach of game theory in heterogeneous network to reduce transmit power and flexible deployment of nodes in dense areas.*

Key Words: Mobile ad hoc network, Intrusion Detection System, Energy efficiency, Mobile nodes, Heterogeneous network.

1. INTRODUCTION

A Mobile ad hoc network (MANET) is a network consists of infrastructure-less framework containing mobile nodes that are connected wirelessly. Each nodes in a MANET acts as host as well as router. In MANET, the communication among nodes is done by establishing dynamic link between source and destination. This link may be unidirectional, bidirectional or omni directional forming a temporary network structure. The transmission of packets from source to destination takes place through intermediate nodes by hopping techniques. MANETs are a kind of ad hoc network where it maintains a highly dynamic and autonomous network topology. Nodes of MANET can be able to move in different direction and can add other mobile nodes frequently forming a dynamic topology. Though MANETs have surplus things, they have some security issues that will cause severe damages and loss in network.

Random linking of mobile nodes leads to add malicious nodes in the network accidentally. To suspect and detect the malicious activity in the network, Intrusion Detection System (IDS) are implemented to analyze the behavior of the neighborhood nodes. Intrusion detection system is a software program, which scans the node for any abnormal behavior. IDS sits on each node in the network to identify the intruder. IDS keeps an eye on every node in the network to observe the behavior and nature of active nodes in the network. However, keeping IDS active at all time in all nodes makes the mobile nodes results in energy loss and high usage of computational resources. This will turn out to be a costly overhead.

IDS mainly focus on encountering the malignant nodes and provide security for safe transmission of packets. By doing so, IDS are categorized into following types: (a) Active IDS, (b) passive IDS, (c) Network IDS, (d) Host IDS .In Active IDS, the nodes in the network are organized in the way that it can automatically intercept the attack without requiring permission from the operator whereas Passive IDS monitors and distinguish the behavior of nodes by analyzing network traffic and it alarms the user about the attack. A Network Intrusion Detection System consists of sensors working in promiscuous mode in which it is placed along the network boundary to analyze the traffic. A Host Intrusion Detection System runs only on individual working nodes in the network. Host IDS monitors the nodes and notifies the operator if any malignant action is detected. The proposed probabilistic model deals with the network based IDS detection in heterogeneous network.

Among various researches in MANET, Only considerable results are highlighted in maintaining the efficiency of mobile nodes in the dynamic network .We consider this issue and derive a probabilistic approach to maintain the energy efficiency and security of MANET in heterogeneous network. The existing model addresses the resource efficiency in homogenous network where our work demonstrates the energy efficiency and security in heterogeneous environment. A Heterogeneous network consists of different types of access nodes in wireless network that are connected in dynamic manner. The proposed approach makes the nodes of MANET to conserve energy and to check the abnormal intrusion in the heterogeneous network.

1.1 Game Theoretic Analysis

A Cooperative game model approach is implemented to analyze the profitable approach in saving energy. Saving Battery power will be subjected as main objective. Each player (IDS) is to monitor the neighbor nodes activity at security level in order to detect malicious activity. In Cooperative modeling, players coordination in attaining their goal is mandatory. Game theory is widely used for modeling IDS in wireless networks.

1.2 Intrusion Detection System

IDS mainly focus in detecting intrusion in heterogeneous network. It is difficult to detect intrusion in MANET because of their infrastructure-less nature. IDS describes suspected intrusion once it has taken and signals an alarm and also watch for the attack that originate from the system. Once an attack is identified or it senses any abnormal behavior, alert can be sent to admin. Signature based and Anomaly based are the two major detection method handled in IDS.

2. PROPOSED WORK

The proposed work attempts to bring forward the energy efficiency as a major factor in MANET. In our work, we derive a distributed scheme of probabilistic model approach to detect the intrusion among nodes by setting a desired security level. Though heterogeneous network consists of nodes in different range and having different computational power, establishment of links for communication among nodes takes place similarly as present in homogenous nodes. The proposed work handles the security and energy conservation in MANET by implementing Heterogeneous Least Degree K method (HLDK).

HLDK is implemented in collection of different nodes that forms a temporary network. IDS is deployed in each node in the network where IDS monitors the neighborhood nodes activity independently. The audit of IDS depends upon the security level that is designed earlier. The Security level depends upon number of neighborhood nodes that monitors a node in a network at any instant of time. The security level also offers a trade-off between security and energy consumption. Large number of neighbors monitor a node at a time serves a higher security level. This may result in higher energy consumption. Each neighbor in the network monitors independently with an optimal probability.

The HLDK mechanism is employed by each node to figure out the least monitoring probability in the network. The algorithm works as follows: Assume a node N which has m neighbors (IDSs).Each node (says N) starts this algorithm by determining the probability. Node N advertises its degree to other nodes within one hop limit. The neighbors of N reply back with their respective degrees. The minimum of those degree will be assigned to m and minimal probability be calculated.

$$\mathrm{TV} \leq \sum_{j=s}^{m} \binom{m}{j} p^{i}(1-p)^{m-j}$$

Where TV represents threshold value which is the minimal probability with which the desired security level(s) is maintained. The value of threshold value can be set depending on application scenario.

If the security level which is already predefined in a network is larger than the assigned m then the minimal probability be 1. Otherwise, Minimum probability of node N be assigned. There will be a chance for the intruder nodes to disrupt the network behavior by sending false degree .Malicious node will more likely to send high degree .HLDK accepts only minimal probability of the node so highest degree will not be chosen. Even if several malicious neighbors collude and report an inflated high degree, if at least there is one honest neighbor that reports correctly, the honest nodes degree will be chosen as minimal degree. It is more secure to decide that at least one neighbor is honest. If malicious node force a node to accept its high degree it will be overcome by analyzing the degree of outlier lower end nodes to identify the false degree of very low value. This case will be aroused only if there is any suspicious activity when neighbor nodes return their degrees to the requested node.

2.1 Analysis of Proposed Scheme

In this division ,the analysis of related approaches of heterogeneous network in the light of various requirements like Effectiveness, Energy Consumption, Computational Cost, Performance evaluation are attempted.

2.1.1 Performance Evaluation

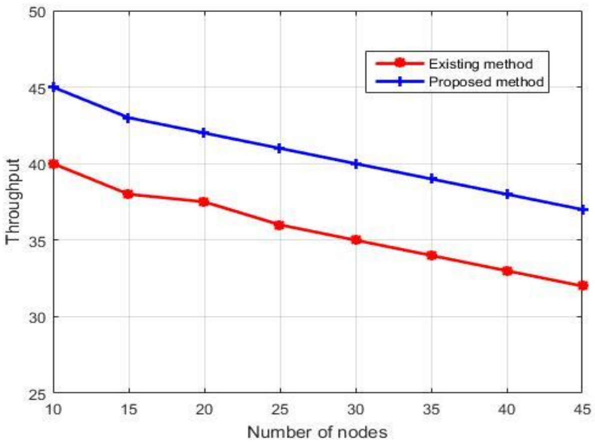

Chart-1: Performance Evaluation

Running IDS all time on the nodes throughout the simulation time will make the network to consume high energy. Hence HLDK is used to reduce the active time of IDs in the network. The detection process of IDS is strict in the sense if s nodes are monitoring a network, at least *s* message are required to convict a malignant node is detected. The results of simulation shows the connection established within its radio range will start at the beginning of simulation and continue till the end without having any degradation. The performance of HLDK almost gives the same result even if HLDK is not implemented in the network.

2.1.2 Effectiveness

The Detection rate decreases as security level increases. In high security level, more number of message will be required to commit a node is a benign node. Detection rate be identified as ratio of number of times benign nodes are detected to the total number of times they should have been detected. Then, High packet drop will be analyzed due to high network density and considerable amount of traffic in the network. Hence detection rate, collision of packets does not affect the effectiveness of HLDK.

2.1.3 Energy Consumption

The nodes are mobile and the degree keeps changing in the network. Node which finds themselves in denser areas of the network will monitor with a high probability than those in less denser areas and consequently will expend more energy. Energy consumption does not make an issue in evaluating HLDK.

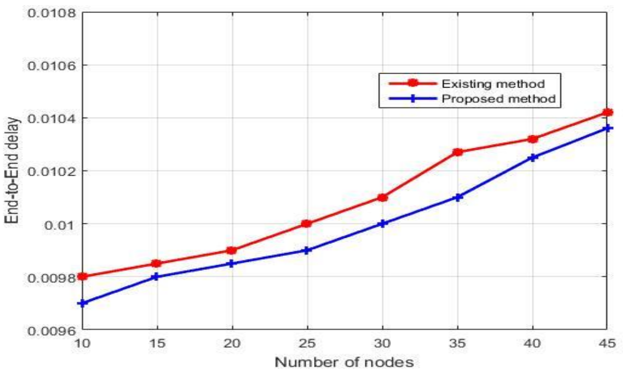

Chart-2: Energy Consumption

2.1.4 Computational Cost:

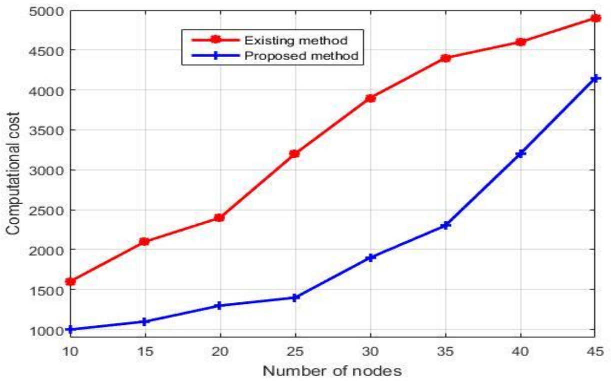

Chart-3: Computational Cost

The computing power spent by IDS will reduces considerably when HLDK is invoked. The computing power spent by IDS depends upon the number of packets received. The number of packets received when HLDK runs in the network is less irrespective of all speed values. This results in saving of computational power.

3. CONCLUSION

In this paper, the proposed approach efficiently showcases the effective energy conservation in heterogeneous network. Another remarkable highlight of the proposed scheme is reducing the active time of IDS running in the nodes. Here, the primary goal is to monitor the nodes activity at desired security level where the secondary is to conserve as much energy as possible. To achieve this, probabilistic approach is implemented, so that optimal probability of node to be set. The efficiency of the proposed scheme is done by i) active running of IDS throughout the simulation time ii) using proposed to reduce the IDS active time in the network. While using the proposed scheme there is considerable reduction of energy in each of the nodes that increases the network lifetime significantly.

REFERENCES

[1] Y. Paul Brutch & Kelvin Ko, Challenges in Intrusion Detection for wireless Ad-hoc Networks, Network associates Laboratory.

[2] D. Dong, X. Liao, Y. Liu, C. Shen and X. Wang, ”Edge Self-Monitoring for Wireless Sensor Networks,” IEEE Transactions on Parallel and Distributed Systems,” vol. 22, no. 3, March 2011, pp. 514-527.

[3] I. Khalil, S. Bagchi and N. B. Shroff,”SLAM: Sleep-Wake Aware Local Monitoring in Sensor Networks,” Proc. 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, 2007 (DSN 2007), 565-574.

[4] Ningrinla Marchang and Raja Datta, ”A Novel approach for efficient usage of Intrusion detection System in Mobile Ad hoc Networks”vol.66,NO.02,Feb 2017

[5] S. M. Fitaci, K. Jaffres-Runser and C. Comaniciu,” On modeling energy security trade-offs for distributed monitoring in wireless ad hoc networks,” Proc. Military Communications Conference, 2008. MILCOM 2008. IEEE, vol., no., pp.1-7, 16-19 Nov. 2008.

[6] Adnan Nadeem and Michael P. Howarth, Protection of MANETs from a range of attacks using an intrusion detection and prevention system, Telecommunications System Journal Springer 52(4) (2013)2047-2058.

[7] F. Li, Y. Yang and J. Wu,”Attack and Flee: Game-Theoretic-Based Analysis on Interactions among Nodes in MANETs,” IEEE Transactions on Systems, Man, and Cybernetics-Part B: Cybernetics, vol 40, no. 3, June 2010, pp. 512-622.

[8] S. Shen,”A game-theoretic approach for optimizing intrusion detection strategy in WSNs,” Proc. 2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC), pp.4510-4513, 8-10 Aug. 2011.

[9] L. M. Feeney, ”Investigating the Energy Consumption of an IEEE 802.11 Network Interface,” Technical Report, ISRN: SICS-T-99/11-SE, ISSN 1100-3154, Swedish Institute of Computer Science, www.sics.se/ lmfeeney

[10] W. Wang, M. Chatterjee, K. Kwiat, and Q. Li. A game theoretic approach to detect and co-exist with malicious nodes in wireless networks. Computer Networks, 71:63–83, 2014.

[11] Eitan Altman and Tania Jimenez, “NS simulator for beginners”,http://www.isi.edu/nsnam/ns/ns-contributed.html, pp. 1-146, 4 December 2003.

[12] N. Stakhanova, S. Basu, J. Wong, A cost-sensitive model for preemptive intrusion response systems, in: Proc. IEEE 21st International Conference on Advance Networking and Applications (AINA), IEEE Computer Society, 2007.

[13] Sandeep J & Satheesh Kumar J 2015, ‘Efficient Packet Transmission and Energy Optimization in Military Operation Scenarios of MANET’, Elsevier, Procedia Computer Science, vol. 47, pp. 400-407.

[14] G. Thamilarasu, et al., A cross-layer based intrusion detection approach for wireless ad hoc networks, in: IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, 2005.

[15] S. Banerjee, S. Khuller, "A Clustering Scheme for Control in Wireless Networks", in Proceedings INFOCOM, 2001.