Energy Efficient Intrusion Detection System in Mobile Ad-Hoc Network

Harshal Bipibhai Tandel[1], Mrs. Sumitra Menaria[2]

[1] Student, Information Technology, Parul Institute of Engineering and Technology, Gujarat, India
[2]Assistant Professor, Computer Engineering, Parul Institute of Engineering and Technology, Gujarat, India,

Abstract

The main characteristics of ad hoc networks are the lack of predefined infrastructure and the dynamic topology. Usually, security in ad hoc networks is handled through intrusion detection system. Each node has its own IDS (intrusion detection system). If all node start its IDS for detection then overall energy consumption will increase as well as lifetime of ad-hoc network will decrease. To balance the resource consumption among all nodes and prolong the lifetime of MANET, nodes with the most remaining resources should be selected as the cluster head. However, there are two main obstacles in achieving this goal. First, without incentives for serving others, a node might behave selfishly by lying about its remaining resources and avoiding being selected. And second, any node joins or leaves the cluster how detection service will carried out. To address the issue of selfish nodes, presenting a solution based on reputation and impact factor value in time shared fashion. For detection watchdog intrusion detection and prevention technique is used.

Keywords - Intrusion *Detection System, Watchdog, Impact Factor, Cluster*

INTRODUCTION

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. Intrusion Detection System is the one of the promising way which provides the security in mobile ad-hoc networks.

RELATED WORKS

An extensive literature survey was done before making

any kind of assumption in our work. In [6] different types of intrusion detection techniques are listed and use of each techniques in different scenario. Marjan Kuchaki Rafsanjani, Ali Movaghar, and Faroukh Koroupi have shown a basic guideline for malicious nodes stop the operation of a routing protocol by changing the routing information or by structuring false routing information. And also Selfish nodes can intensively lower the efficiency of the network since they do not easily participate in the network operations. In [4] this paper Chuan-xiang Ma , Ze-ming Fang, Lei-chun Wang and Qing-hua Li have used four different modules named resource management, monitoring state management, local detection, network detection. Here ETBAS is an adaptive selection scheme and adaptable to dynamically changing networks more flexible architecture with alterable network detection is designed each node with the same IDS has an equal opportunity to be selected as monitoring node on activating its network detection model, which is helpful to efficiently utilize the limited network energy resource to enhance the network lifetime. In

[7] Ningrinla Marchang and Rakesh Tripathi have used two different techniques named perfect IDS and imperfect IDS. In this paper a two-player non-cooperative game for modeling interactions between intrusion detection systems (IDS) and an attacker in Mobile Ad hoc Network is presented. They used the game to deter- mine whether it is essential to always keep the IDS running with- out compromising on its effectiveness. The results of this model show that it is indeed not required to keep the IDS running all the time while maintaining its effectiveness. IT also helps in determining the optimal defense strategies that the network administrator must deploy. In [8] M. Hossein Ahmadzadegan, M. Ehnusrati and Augie Widyotriatmo have used different modules of units named security analysis unit, attack database unit, detection unit, intrusion detection unit, and backup and storage unit. Here less energy consumption alternative is provided and proves the effectiveness and efficiency of the proposed IDS due to considerations of a less amount of processing cycles and more integration during the design. In [2] Santosh kumar Sabat and Sujata Kadam have used three different techniques named reputation system model, leader election process, cost of analysis Function . This paper used reputation based leader election algorithm, along with adaptive energy scheme for conserving the energy of nodes. To give a secure solution and also selfish node will be inspired to honestly participate in the election process. Here the performance parameter such as percentage of alive nodes, residual energy of nodes and shown that how energy is conserved in adjusted transmission range scheme and the nodes serve the system for longer duration.

SYSTEM MODEL AND ASSUMPTION

In mobile ad-hoc networks each node has unique identity (ID) and its energy level. This is considered as private information for every node.And cluster head selection process is also dependent on node's energy level. By using this approach there are several problems to be considered.

- Nodes may reveal fake information about its energy for not participating in detection process. If node reveals its true value than the node which has least energy level has highest chances of being attacked.
- Nodes may add or remove from cluster then how intrusion detection service provides to cluster.

So propose a solution for balancing the resource consumption of IDSs among all nodes while preventing nodes from behaving selfishly. To address the selfish behavior, design cluster in the form of reputation to motivate nodes to honestly participate in the selection scheme by revealing their Impact Factor. The Impact factor is designed to protect nodes' private information (energy level) and ensure the contribution of every node on the selection process. For detection cluster based intrusion detection and prevention technique is used.

SYSTEM MODEL AND ARCHI TECTURE

Impact Factor Calculation:

Impact Factor is designed based on node's Residual Energy, number of Participation and number of neighbor nodes.

And each node have Impact Factor **IF_i=**

Where REi=Residual energy of i
NEi=Number of neighbors nodes i have
PTi =Number of times node i have participate in detection process

Steps:

1] Initially each node has its residual energy, number of participation and number of neighbor nodes. When hello massage received by each node calculates its impact factor IF and reply.

2] After verify its neighbor's impact factor each node send vote for least impact factor value choose the node as cluster head.

3] After getting highest votes node accept cluster head and send acknowledge to all nodes in cluster.

4] It will launch its IDS for particular time slot and provide service to other nodes in cluster.

[A] For cluster Head selection work flow diagram

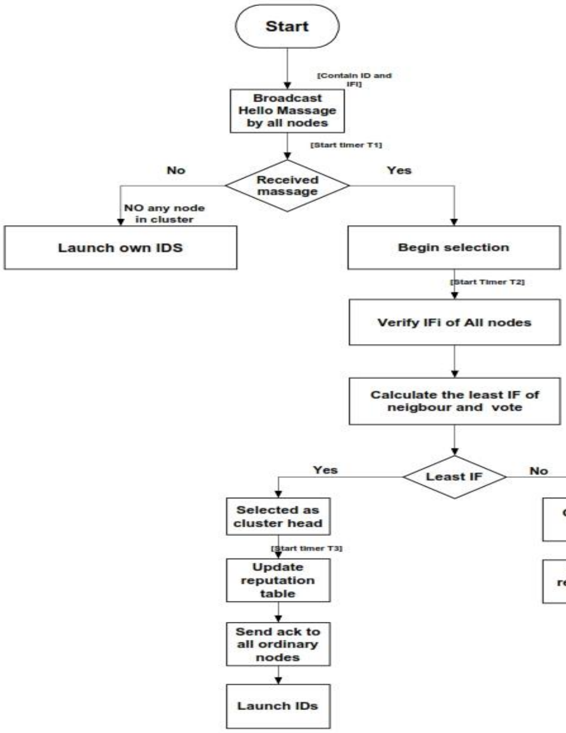


Fig: 1. work flow diagram of cluster head selection

[B] Example

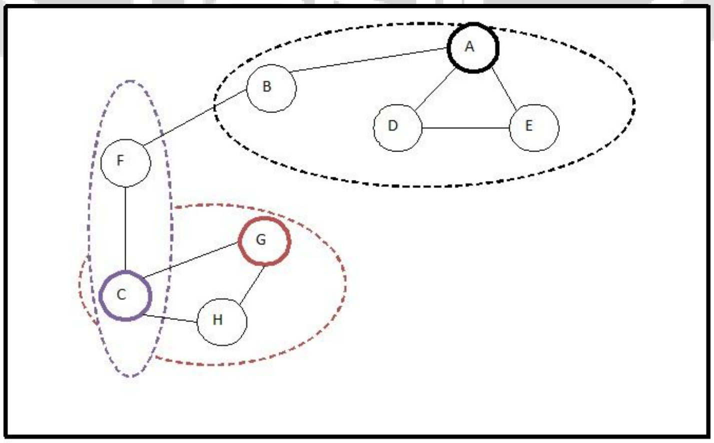
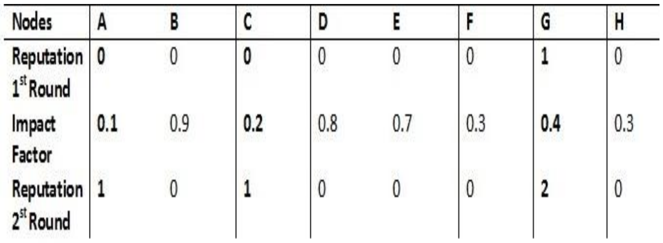


Fig: 2. Cluster head selection in different clusters

In above figure there are three groups of clusters. Each cluster has some mobile nodes and darker round indicate the cluster head of the cluster.

Here node A, C and G node selected as cluster head because of least impact factor. The reputation of node is initially 0 and 1. After providing service reputation value of cluster head will increment and the other node's reputation value will be as it is. Here normal nodes will motivate to provide service and increase its reputation value.

Table: 1. Example



Nodes	A	B	C	D	E	F	G	H
Reputation 1st Round	**0**	0	**0**	0	0	0	**1**	0
Impact Factor	**0.1**	0.9	**0.2**	0.8	0.7	0.3	**0.4**	0.3
Reputation 2st Round	**1**	0	**1**	0	0	0	**2**	0

[C] Detection process:

watchdog method is a strategy that detects misbehaving nodes acting alone by maintaining a buffer that contains recently sent packets. When a node forwards a packet, the node's watchdog ensures that the next node in the path also forwards the packet. The watchdog does this by listening all nodes promiscuously. If the next node does not forward the packet then it is termed as misbehaving. In this scheme, every packet that is overheard by the watchdog is compared with the packet in the buffer to see if there is a match. A match confirms that the packet has been successfully delivered and it is removed from the buffer. If a packet has remained in the buffer beyond the timeout period, then a failure counter for the node responsible for forwarding the packet is incremented. If this counter exceeds a predetermined threshold then the node is termed as malicious and the network is informed accordingly by a message sent by the node that detects the problem.

SIMULATION RESULTS

The scheduling algorithm was simulated using the ns22.34

Simulator. Various realistic radio ranges were taken where the nodes move according to the way-point mobility model with a maximum speed of 10 m/sec. The pause time used was 2 seconds and the routing protocol used was Ad hoc On demand Distance Vector (AODV) [1]. The IDS technique used here is watchdog.

We ran the simulation for different number of nodes N. Here in first simulation we have take different energy consumption by number of nodes 5, 10, 15, 20, 25 without creating cluster. After then we have simulate nodes with formation of different cluster for group of nodes for example 5. For each value of N, we used different movement space. [1]The percentage of collision was calculated using total number of messages sent and actual number of messages received. If there were no collision, the actual number of messages received is equal to the total number of messages sent. However, when collisions were assumed, actual number of messages received was less than the total number of messages sent [1].

The most important part of our algorithm is to decrease the average energy decay rate of the network. In Fig 3 we have shown the average energy consumption of different values of nodes with cluster and without cluster formation in the network. When there is no cluster formation of nodes means there is no scheduling. All the nodes run their IDS

at the same time[1]. As all the nodes run their IDS at the

same time, the average energy consumption is significantly

Higher in comparison to cluster with higher value of nodes.

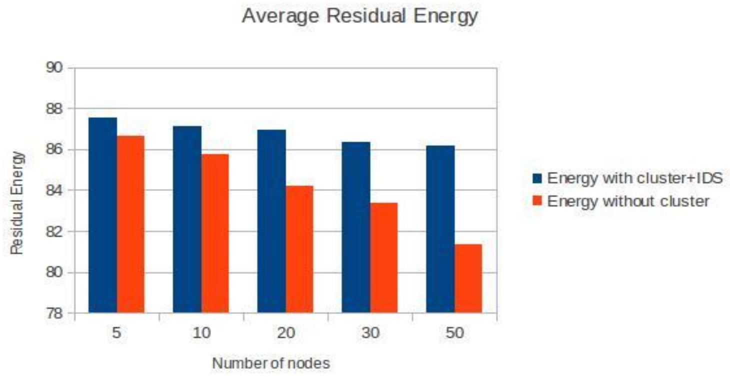


Fig.: 3. Average Energy consumption Ratio

In above figure movement space taken for simulation is 1000m*1000m. Each node initially provided 100J energy. When number of nodes increase without cluster formation average energy consumption rate is more than with cluster of nodes.

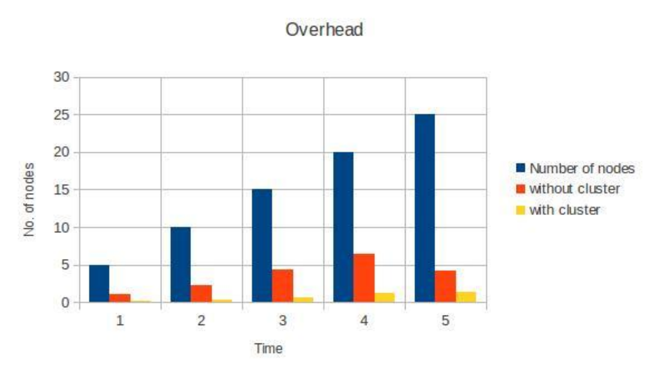


Fig.: 4. Message overhead

In mobile ad-hoc network intrusion detection system store the table of neighbor nodes. So while number of nodes increase in the network massage overhead will also increase. By applying clustering in network massage overhead decreased compared to without cluster in network.

CONCLUSION

Energy is most powerful constraint of MANET. So for that optimum selection of cluster head and provide security for entire cluster in energy efficient manner. Here proposed energy efficient algorithm provide cluster based intrusion detection where average energy consumption decrease as per without cluster of nodes and message overhead also decreased. This kind of applications used in rescue mission for example natural disasters earthquake, flood etc where communication have first priority and security comes further. So for maintain energy we have proposed cluster based algorithm for mobile ad-hoc networks.

REFERENCES

[1] Bapi Kisku and Raja Datta Member, IEEE “An Energy Efficient Scheduling Scheme for Intrusion Detection System in Mobile Ad-hoc Networks” 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing.

[2] Santoshkumar Sabat, Sujata Kadam, IEEE 2014 “Adaptive Energy Aware Reputation Based Leader election for IDS in MANET” International Conference on Communication and Signal Processing, April 3-5, 2014, India

[3] Noman Mohammed, Hadi Otrok, Lingyu Wang, Mourad Debbabi, and Prabir Bhattacharya, Fellow, IEEE 2011. “Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET” Ieee Transactions On Dependable And Secure Computing, Vol. 8, No. 1, January-February 2011

[4] Chuan-xiang Ma , Ze-ming Fang, Lei-chun Wang and Qing-hua Li ,2009 “A Novel Intrusion Detection Architecture for Energy-Constrained Mobile Ad-hoc Networks” 2009 International Conference on Multimedia Information Networking and Security .

[5] K. Komathy , P. Narayanasamy ,2007 “A Probabilistic Behavioral Model for Selfish Neighbors in a Wireless Ad Hoc Network” IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.7, July 2007.

[6] Marjan Kuchaki Rafsanjani, Ali Movaghar, and Faroukh Koroupi, 2008 “Investigating Intrusion Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes” World Academy of Science, Engineering and Technology 44 2008.

[7] Ningrinla Marchang and Rakesh Tripathi, 2009 “A Game Theoretical Approach for Efficient Deployment of Intrusion Detection System in Mobile Ad Hoc Networks” 15th International Conference on Advanced Computing and Communications.

[8] M. Hossein Ahmadzadegan, M. Ehnusrati and Augie Widyotriatmo “WiMAX-Based Energy Efficient Intrusion Detection System” 2013 International Conference on Robotics, Biomimetics, Intelligent Computational Systems (ROBIONETICS) Yogyakarta, Indonesia, November 25-27,2013.

[9] Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE,2013 “EAACK—A Secure Intrusion-Detection System for MANETs” Ieee Transactions On Industrial Electronics, Vol. 60, No. 3, March 2013.

[10] Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker 2000 “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks” ACM 2000.

[11] Dr. Mohammad U. Bokhari ,Hatem S. A. Hamatta Shams, Tabrez Siddigui ,2012 “A Review of Clustering Algorithms as Applied in MANETs” International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 11, November 2012.

[12] Yacine Rebahi, Vicente .E Mujica-V, Dorgham Sisalem,2005 “A Reputation-Based Trust Mechanism for Ad hoc Networks” Proceedings of the 10th IEEE Symposium on Computers and Communications (ISCC 2005)

[13] Dr. B. Paramasiva, K. Mohaideen Pitchai “Modeling Intrusion Detection in Mobile Ad Hoc Networks as a Non Cooperative GAME” Proceedings of the 2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME) February 21-22.

[14] Nithya Karthika , Raj Kumar “Survey on Network Based Intrusion Detection System in MANET”, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.4, April- 2014, pg. 660-663.

[15] Sudarshan Vasudevan, Jim Kurose, Don Towsley "Design and Analysis of a Leader Election Algorithm for Mobile Ad Hoc Networks" Proceedings of the 12th IEEE International Conference on Network Protocols (ICNP'04)

[16] Anitha Julian, A.Pravin Renold, V.Kalpana, C.P.Koushik "E-Lanmar: Energy Aware Landmark Selection for Mobile Ad hoc Networks" 2013 International Conference on Computer Communication and Informatics (ICCCI -2013), Jan. 04 – 06, 2013, Coimbatore, INDIA.

[17] Hadi Otrok, Noman Mohammed, Lingyu Wang, Mourad Debbabi and Prabir Bhattacharya "A Moderate to Robust Game Theoretical Model for Intrusion Detection in MANETs" IEEE International Conference on Wireless & Mobile Computing, Networking & Communication

[18] Noman Mohammed, Hadi Otrok, Lingyu Wang, Mourad Debbabi and Prabir Bhattacharya "A Mechanism Design-Based Multi-Leader Election Scheme for Intrusion Detection in MANET" IEEE Communications Society subject matter experts for publication in the WCNC 2008.

[19] Debdutta Barman Roy, Rituparna Chaki, Nabendu Chaki "A New Cluster-Based Wormhole Intrusion Detection Algorithm For Mobile Ad-Hoc Networks" International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 1, April 2009.

[20] Luzi Anderegg, Stephan Eidenz "Ad hoc-VCG: A Truthful and Cost-Efficient Routing Protocol for Mobile Ad hoc Networks with Selfish Agents" ACM MobiCom'03, September 14–19, 2003, San Diego, California, USA.

[21] Mohammad Wazid, RHGoudar and Avita Katal "Cluster and Super Cluster Based Intrusion Detection and Prevention Techniques for JellyFish Reorder Attack" 2012 2nd IEEE International Conference on Parallel,D istributed and Grid Computing.