Threshold Based Intrusion Detection System for MANET using Machine Learning Approach

[1]Sapna Choudhary, [2]Alka Agrawal

Deptt. of Computer Science & Engineering
Shri Ram Group of Institute, JABALPUR, INDIA
Emailid:choudharysapnajain@gmail.com, agrawal132@gmail.com

Abstract: *Adhoc nature of Mobile Adhoc Network makes MANET most promising communication model in rescue and military areas. Its dynamicity property and infrastructure less deployment invites attacker (insider or outsider) to disrupt the MANET. Hosts itself as a router makes cooperation better but finding the route has inherent weakness which is beneficial for intruders to declare authenticate itself in MANET. On demand routing protocols such as AODV works well in context MANET consequently targeted for attack for the intruders. Various mechanisms has been proposed since the evolution of the MANET having their own pros and cons. Author [1] has depicted the solution for the black hole (BH) and gray hole of both type towards source and destination. Both the attacks are most common and harmful in MANT scenario. Author has adopted the concept of threshold mechanism applying on packet drop metrics to calculate maliciousness locally (by each node) using fuzzy logic. Author has consider only metrics for its evaluation i.e. packet drop ratio. In this article we have proposed a more enhanced method to detect intrusion by integrating more metrics like packet delivery ratio, routing overhead and author's packet drop ratio to calculate the suspiciousness of the node with the help of machine learning approach to classify the nodes whether they are authenticated or intruders. Proposed mechanism has been implemented on NS-3.18 on AODV routing protocols and machine learning tool. Obtained results are better than existing method with ease of simplicity and accuracy.*

Keywords:*NS-3,MANET,AODV*

I. INTRODUCTION

The Mobile Ad-Hoc Networks are autonomous and decentralized wireless systems. MANETs consist of mobile nodes that are free in moving in and out in the network. Nodes are the systems or devices i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer that are participating in the network and are mobile. These nodes can act as host/router or both at the same time. They can form arbitrary topologies depending on their connectivity with each other in the network. These nodes have the ability to configure themselves and because of their self configuration ability, they can be deployed urgently without the need of any infrastructure. Internet Engineering Task Force (IETF) has MANET working group (WG) that is devoted for developing IP routing protocols. Routing protocols is one of the challenging and interesting research areas. Many routing protocols have been developed for MANETS, i.e. AODV, OLSR, DSR etc.

Security in Mobile Ad-Hoc Network is the most important concern for the basic functionality of network. The availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANETs often suffer from security attacks because of its features like open medium changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANETs against the security threats.

The MANETs work without a centralized administration where the nodes communicate with each other on the basis of mutual trust. This characteristic makes MANETs more vulnerable to be exploited by an attacker inside the network. Wireless links also makes the MANETs more susceptible to attacks, which make it easier for the attacker to go inside the network and get access to the ongoing communication [9, 21]. Mobile nodes present within the range of wireless link can overhear and even participate in the network.

MANETs must have a secure way for transmission and communication and this is a quite challenging and vital issue as there is increasing threats of attack on the Mobile Networks. Security is the cry of the day. In order to provide secure communication and transmission, the engineers must understand different types of attacks and their effects on the MANETs. Wormhole attack, Black hole attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service (DoS), selfish node misbehaving, impersonation attack are kind of attacks that a MANET can suffer from. A MANET is more open to these kinds of attacks because communication is based on mutual trust between the nodes, there is no central point for network management, no authorization facility, vigorously changing topology and limited resources.

The routers in MANETs move freely, in any direction or speed, and are allowed to organize themselves arbitrarily. Such members make such a network ”non-engineered” - the network topology changes dynamically and unpredictably. There is no fixed infrastructure, and this results in nodes willingly forwarding data to any other node, often in a peer-to-peer, multi-hop mode. MANETS possess a need to dynamically determine routing based on availability or visibility of nodes. MANETs also have nodes whose energy storage is very limited. Often, they are battery equipped, with very limited to no recharging or replacement possible.

Conserving energy while trying to run normal operations is a huge factor in the design and implementation on MANETs. Another limited resource in MANETs in bandwidth. To cope with the energy and bandwidth requirements, MANETs employ grouping techniques, in which some nodes perform specific functions (like forwarding/relaying sensor data), while more powerful members perform more resource-intensive activities (like data aggregation, routing etc). As some nodes die, or are put out of service, other nodes shoulder responsibilities. Thus, often, MANETs are heterogeneous networks, with varying member profiles and a varying count of members.

All of the above features of MANETs pose a serious challenge in what is often easier to achieve or predict in wired or infrastructure based networks. Guaranteeing data safety and reliability is a serious concern. Thus, the decentralized nature, scalable setup and dynamically changing topology makes adhoc networks ideal for a variety of applications ranging from front-line zones(military, industrial and natural) to data collection(machinery analysis, biosensing) as investigated in [2]. But the same features drive the key challenges in deploying and using them: device compatibility, connectivity issues due to varying traffic profiles, security and survivability.

II. RELATED WORK

Due to highly dynamic nature topology in MANET makes routing procedure more complicated and insecure and therefore nodes are more susceptible to compromise and are particularly vulnerable to denial of service attack (DoS) attacks launched by [1] malicious nodes or intruders. Hence routing is [2] more complex and insecure. The wireless nodes are prone to compromise and vulnerable to various types of attacks like DoS (denial of Service), wormhole attack, flooding, green hole attack, black hole attack and selfish node attack. These all are affect the performance of MANET. Denial of service (DoS) attacks commence by intruders to prevent the service being used by legitimated users. Route request (RREQ) is one of flooding attack [3] [4] launched by nodes in distributed manner in such a aim that compromised node can takes benefit of the route discovery process and floods the entire network by propagating huge number of fake route request (RREQs) consequently [18] network is jammed leading to a denial of service.

Abderrahmane Baadache and Ali Belmehdi [4] address the importance of security in MANET. According to authors [6] securing of MANET is make sure mutual authentication of participants nodes, confidentiality and integrity of exchanged data, availability of the network resources, access control to the communication medium and the anonymity.

According to Authors of [7] MANET attacks generally includes attempting to drop or modify packets, gaining authentication or procuring authorization by inserting false packets into data stream.

Various types of attacks has been identified some of them are discuss below-

A) Denial of Service Attack (DoS) [2]

The another variation of the DoS is Flooding Attack The Flooding Attack is a denial-of-service attack in which malicious nodes which malicious node sends the useless packets to consume the valuable network resources. Flooding attack is possible in[8][9] all most all on demand routing protocol.

B) Routing table overflow

C) Impersonation

A node may perhaps impersonate another node and send false routing information masqueraded as some other normal node.

D) Power consumption

E) Information disclosure

In mobile ad hoc networks, packets with information including status of a node, location, private or secret keys and passwords, are easily eaves dropped due to the nature of broadcast.

F) Packet modifying

When an intermediate node modify the contents of packets while transmission.

G) Selfish Node

Selfish nodes are those which save their resources by not taking part in communication.

H) Black hole

It is a kind of selfish node that just drops the packets [10] and hence the transmission further . A malicious node diverts the destination by sending incorrect RREP (route reply) that it has a latest route with minimum hop count to destination and then [11] it drops all the receiving packets.

I) Gray Hole

In Gray Hole Attack [12] a malicious node drops the packet and does not forward them. Gray Hole attack can be act as a slow poison in the network side that is the probability of packet loss is undetermined [13] [14].

J) Worm Hole

A worm hole attack is when two or more malicious nodes may collaborate to encapsulate and exchange messages between them along existing data routes . A worm hole reflects the route that may seems fine to the destination but it always tunnels the packet to its malicious partner node. This attack is also [15] known as tunneling attack.

Many methods has been proposed to solve the wormhole detection and prevention author of has review and addresses a technique based on a variant of the counting technique in which nodes broadcast group of hashes of the packets received out of last k time intervals.

Author of [2] has found that Ad hoc network and its applied in to topology among nodes are extremely dynamic in nature (unstable due to mobility),in such scenarios the routing process is to be more [16] complicated and anxious.

Another prospect about wireless operated devices or nodes are they are very much prone to compromise. Specifically they are the first choice of target of attacker for DoS attack.

Denial of service (DoS) (also called flooding) is two types control and data flooding. Control flooding is also called RREQ flooding [17] [18] in which excess number of RREQ is flooded in the adhoc network that prevents other node to access the services. When set of suspicious nodes are generate excess number of RREQ request it is termed as Distributed Denial of Service (DDoS) attack in which a compromised node takes benefit of the route discovery mechanism of on demand routing protocols of MANET and jam (floods) the entire network through transmitting huge number of forged RREQs to fictional nodes in the network and leading to a denial of service [19] attack.

Most of the security related MANET research is centered in around AODV routing protocols. In this article we are going to evaluate the impact of the flooding attack in DSR on demand routing protocols.

Hence Flooding attack has become a major security concern in [19] recent years. It is the novel research area since last three years because none of the existing methods are proposed so far detecting and controlling of the impact of flooding in wireless or MANET in practical aspect.

Everything has two sides, pros and cons. Mobile adhoc offers instant solution for communication when requires without establishing infrastructure with wireless mobility feature. MANET is a kind of automatic networks which composed of flexible, dynamic, and fully autonomous network entities that can (re)systematize in accordance with the operational, cost-effective, and societal needs of the users and organizations .

Although MANET offers quick and fast communication environment using atomicity (multihop routing), its application and performance would be spectacularly obstruct in [20] absence of security measure. One of them attack is Denial of Service attack (flooding) launched via taking the advantages of MANET [22] routing concept (flooding in route discovery) and multihop communication.

Although there are lots of convention security approach used in wired network to detect and prevent DoS attack but the main problem with such approach is dynamic nature of MANET because network topology constantly changes.

Hence traditional methods are inefficient.. Another problem is novelty in attacks (intrusion) hence signature based mechanism does not perform well in such scenario.

III. Proposed Work

Mobile Ad hoc network (MANET) is a new paradigm in wireless revolution, which is a self-configured network of wireless mobile nodes. Due to proliferation of miniature yet powerful mobile computing devices, it is gaining acceptance and popularity. However, MANET is vulnerable to security attacks due to its inherent characteristics such as dynamic topology, lack of a centralized coordinator and open wireless channel. In this paper, author analyze some security attacks of MANET and we propose to identify the attack by using an Intrusion Detection System (IDS). The proposed IDS uses fuzzy logic to detect malicious behavior and identify the attacks.

Existing Method:

Author of [1], has found that “While intrusion detection (IDS) technique will work on top of any routing protocol”.

Author had chosen the Ad hoc On-demand Distance Vector (AODV) [6] routing protocol for our experimentation. AODV is design to provide communication between mobile nodes with minimal control overhead and minimal route acquisition latency.

Author’s survey

Due to its inherent characteristics such as dynamically changing topology, weak physical protection of nodes, open wireless access medium, the absence of centralized administration and high dependency on inherent node cooperation, intrusion detection in MANET is a challenging task to say the least. It is extremely easy for malicious nodes, selfish nodes, covert channels and eavesdroppers to bring down the whole network. As a result, MANETs are vulnerable to various attacks and threats.

An Intrusion Detection System (IDS) will undoubtedly be a crucial ingredient in any comprehensive security solution.

The reason behind this is that a prevention mechanism -such as securing a routing protocol using cryptographic primitives - is not a foolproof mechanism. However, designing an effective Intrusion Detection System (IDS) [4], as well as other security mechanisms, requires a deep understanding of the threat model and adversaries attack capabilities. Identifying security attacks is similar in nature to medical diagnosis. Just as several diseases may share some common symptoms but with varying degree, several security attacks may share some common behavior such as dropping of packets with a varying degree. However, a disease may exhibit some special characteristic not seen in other diseases.

Fuzzy logic [1-2] is a computational paradigm that provides a mathematical tool for dealing with the uncertainty and the imprecision that is involved in human reasoning, which is also known as approximate reasoning. The interpretability characteristic of fuzzy logic, which is the capability to express knowledge in a linguistic way, makes fuzzy logic-based systems attractive for applications such as medical diagnosis [7]. Our fuzzy logic-based IDS is based on the system described in [7], which is used to diagnose diabetics.

Author proposed a design for an Intrusion Detection System that detects intrusion in a MANET caused by malicious nodes launching different types of attacks. With the help of fuzzy logic, we tackle three types of routing attacks [5], which exhibit packet forwarding misbehavior, viz., Black hole attack, Gray hole attack towards a source and Gray hole attack towards a destination.

Proposed Method:

Monita Wahengbam and Ningrinla Marchang proposed a fuzzy based IDS method on which he used the concept of threshold to detect 3 types of MANET attack using AODV routing protocol-

1. BLACK HOLE
2. GRAY HOLE
3. Packet Forwarding Misbehavior

Modification required in exiting methods

Following issues are the core element of the proposed work derived from article [1]-

1. Author only talking about 3 attacks. But there is another biggest attack which will also consider for effective design of the IDs i.e. Selfish Node Attack,
2. Authors adopt the idea of fuzzy logic that need to be enhanced, because false rate will increase if threshold value not properly decide.

We will adopt the idea of Machine Learning approach to design full IDS system for the MANET. For this we will use enhanced SVM machine concept distributivly for each node.

3. Routing protocol chosen by the author is good but only AODV alone is not applied everywhere. So we will consider the other routing protocols as well, like OLSR and DSDV for better optimization.

4. Anomaly detection is the best way to detect other unknown (new) types of attack. Our proposed work will adopt the idea of behavioral anomaly detection to design better IDS capability system.
5. It is found that NS-2 patches are not stable they have bugs which will be incompatible for the previous and next future version. So that for better evaluation we will use NS-3.18 which stable and accurate with better test bed option for the network related research and methods especially in wireless scenario.

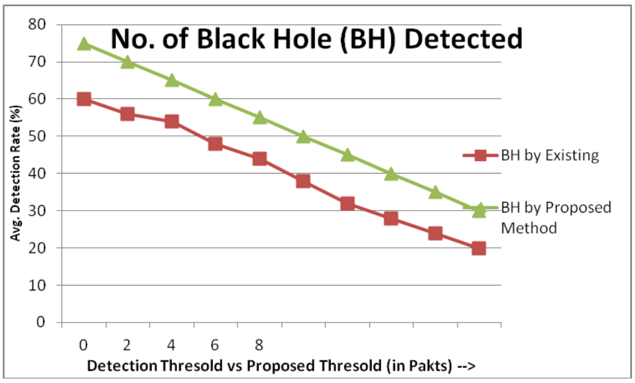
IV. SIMULATION RESULTS

The NS 3 Introduction: ns (from network simulator) is a name for series of discrete event network simulators, specifically ns-1, ns-2 and ns-3. All of them are discrete-event network simulator, primarily used in research and teaching. Ns-3 is free software, publicly available under the GNU GPLv2 license for research, development, and use.

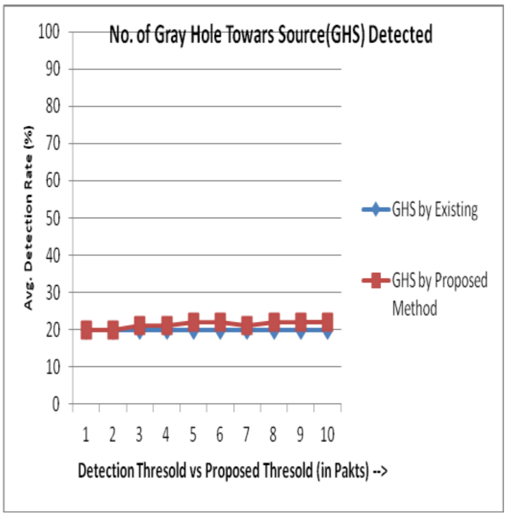
The goal of the ns-3 project is to create an open simulation environment for networking research that will be preferred inside the research community:

- It should be aligned with the simulation needs of modern networking research.
- It should encourage community contribution, peer review, and validation of the software.

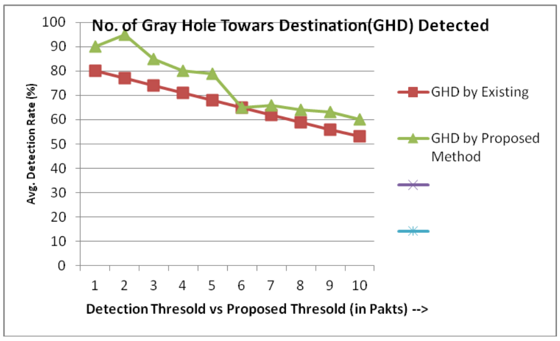
Since the process of creation of a network simulator that contains a sufficient number of high-quality validated, tested and actively maintained models requires a lot of work, ns-3 project spreads this workload over a large community of users and developers.



Fig(a)



Fig(b)



Fig(c)

V. CONCLUSION

Security in MANET is the today's need of effective and secure communication. IDS in MANET has need proper attention to prevent unauthorized attack such as selfish node, black hole and gray hole attack. In this article we have survey the authors proposed the solution for the black hole (BH) and gray hole of both type towards source and destination. Both the attacks are most common and harmful in MANT scenario. Author has adopted the concept of threshold mechanism applying on packet drop metrics to calculate maliciousness locally (by each node) using fuzzy logic. Author has consider only metrics for its evaluation i.e. packet drop ratio. In this article we have proposed a more enhanced method to detect intrusion by integrating more metrics like packet delivery ratio, routing overhead and author's packet drop ratio to calculate the suspiciousness of the node with the help of machine learning approach to classify the nodes whether they are authenticated or intruders. Proposed mechanism has been implemented on NS-3.18 on AODV routing protocols and machine learning tool. Obtained results are better than existing method with ease of simplicity and accuracy.

VI. REFERENCES

[1] Monita Wahengbam and Ningrinla Marchang "Intrusion Detection in MANET using Fuzzy Logic", IEEE, 2012.

[2] Prasenjit Choudhury, Subrata Nandi, Anita Pal and Narayan C. Debnath "Mitigating Route Request Flooding Attack in MANET using Node Reputation", IEEE, 2012.

[3] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks", Proc. of Wireless Communications, IEEE, Oct 2007, Issue 5, pgs 85-91.

[4] R. H. Khokhar, M. A. Ngadi, S. Mandala, "A Review of Current Routing Attacks In Mobile Ad Hoc Networks", International Journal of Computer Science and Security (IJCSS), Volume 2, Issue 3, pp. 18-29, June 2008.

[5] Abderrahmane Baadache and Ali Belmehdi "Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks", Elsevier Journal of Network and Computer Applications 35 (2012) 1130–1139. Availavle at SciVerse ScienceDirect.

[6] J. Lundberg, Routing security in ad hoc networks, in: Proceedings of the Helsinki University of Technology, http://citeseer.nj.nec.com/400961.html.

[7] Alokparna Bandyopadhyay1, Satyanarayana Vuppala, Prasenjit Choudhury, "A Simulation Analysis of Flooding Attack in MANET using NS-3", 978-1-4577-0787-2/11/$26.00 ©2011 IEEE

[8] A.Vani, D.Sreenivasa Rao, "Providing of Secure Routing against Attacks in MANETs",International Journal of Computer Applications (0975 – 8887) Volume 24– No.8, June 2011

[9] Raja Karpaga Brinda .R, Chandrasekar.P , " Detection and Removal of Co-Operative Black Hole\Black Hole Attack in Manet", International Journal of Computer Applications (0975 – 8887) Volume 43– No.11, April 2012

[10] Madhusudhananagakumar KS , G. Aghila, "A Survey on Black Hole Attacks on AODV Protocol in MANET" , International Journal of Computer Applications (0975 – 8887) Volume 34– No.7, November 2011

[11] Vishnu K, and Amos J .Paul," Detection & Removal of cooperative Black/Gray hole attack in Mobile ADHOC Networks." International Journal of

Computer Applications 2010, Volume 1-No.22, pp.38-42.

[12] Onkar V.Chandure, V.T.Gaikwad, “ Detection & Prevention of Gray Hole Attack in Mobile Ad-Hoc Network using AODV Routing Protocol”, International Journal of Computer Applications (0975 – 8887) Volume 41– No.5, March 2012

[13] Jayraj Singh, Arunesh Singh, Raj Shree, “An Assessment of Frequently Adopted Unsecure Patterns in Mobile Ad hoc Network: Requirement and Security Management Perspective”, International Journal of Computer Applications (0975 – 8887) Volume 24– No.9, June 2011

[14] Mahendra Kumar, Ajay Bhushan, Amit Kumar,” International Journal of Advanced Research in Computer Science and Software Engineering”, Volume 2, Issue 4, April 2012.

[15] Muhammad O Pervaiz, Mihaela Cardei and Jei Wu, “Routing security in ad hoc wireless networks”, Department of Computer Science and Engg, Florida Atlantic University, Boca Raton, FL 33431.

[16] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks", Proc. of Wireless Communications, IEEE, Oct 2007, Issue 5, pgs 85-91.

[17] R. H. Khokhar, M. A. Ngadi, S. Mandala, "A Review of Current Routing Attacks In Mobile Ad Hoc Networks", International Journal of Computer Science and Security (IJCSS), Volume 2, Issue 3, pp. 18-29, June 2008. .

[18] Alokparna Banerjee, Satyanarayana Vuppala, Prasenjit Choudhury and Suvrojit Das, “Survey of Flooding Attack Remedies in MANET”, in Proc. of the International Conference on Communication and Broadband Networking (ICCBN 2011), June 2011.

[19] Zonghua Zhang, Farid Naı¨t Abdesselam , Pin-Han Ho and Youki Kadobayashi “Toward cost-sensitive self-optimizing anomaly detection and response in autonomic networks”, Elsevier, computers & security 30 (2011) 525-537.

[20] Meysam Alikhany and Mahdi Abadi “A Dynamic Clustering-based Approach for Anomaly Detection in AODV-based MANETs”, IEEE, International Symposium on Computer Networks and Distributed System (CNDS), Feb 23-24, 2011.