International Journal on Recent Researches in Science, Engineering & Technology (IJRRSET)
A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy. Journal Indexed in JIR, DIIF and SJIF.
Research Paper
Available online at: www.jrrset.com
UGC Approved Journal No: 45483
Received on: 12.11.2017 Published on: 30.11.2017 Pages : 63-69

ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105
Volume 5, Issue 11
November 2017.
JIR IF : 2.54
DIIF IF : 1.46
SJIF IF : 1.329

THRESHOLD BASED INTRUSION DETECTION SYSTEM FOR MANET USING MACHINE LEARNING APPROACH

J.Mahadevan, M.Thavachelvam, S.Niranchana Devi
Dhanalakshmi Srinivasan College of Engineering and Technology, Chennai, India

Abstract

Adhoc nature of Mobile Adhoc Network makes MANET most promising verbal exchange mannequin in rescue and army areas. Its dynamicity property and infrastructure much less deployment invitations attacker (insider or outsider) to disrupt the MANET. Hosts itself as a router makes cooperation higher however discovering the route has inherent weakness which is advisable for intruders to declare authenticate itself in MANET. On demand routing protocols such as AODV works well in context MANET consequently centered for attack for the intruders. Various mechanisms has been proposed in view that the evolution of the MANET having their own pros and cons. It has depicted the answer for the black hole (BH) and gray gap of each kind toward supply and destination. Both the assaults are most frequent and detrimental in MANT scenario. It adopted the thinking of threshold mechanism applying on packet drop metrics to calculate maliciousness regionally (by every node) the use of fuzzy logic. Author has reflect on consideration on solely metrics for its contrast i.e. packet drop ratio. In this article we have proposed a more advantageous technique to observe intrusion with the aid of integrating extra metrics like packet delivery ratio, routing overhead and author's packet drop ratio to calculate the suspiciousness of the node with the assist of desktop studying method to classify the nodes whether they are authenticated or intruders. Proposed mechanism has been implemented on NS-3.18 on AODV routing protocols and computer mastering tool. Obtained outcomes are better than existing method with ease of simplicity and accuracy.
Keywords: AODV , NS-3, MANET.

I. INTRODUCTION

The Mobile Ad-Hoc Networks are autonomous and decentralized wi-fi systems. MANETs consist of cell nodes that are free in shifting in and out in the network. Nodes are the systems or units i.e. mobile phone, laptop, non-public digital assistance, MP3 player and private laptop that are collaborating in the network and are mobile [1]. These nodes can act as host the router or both at the concurrent time. They can form arbitrary topologies relying on their connectivity with every different in the network. These nodes have the capacity to configure themselves and due to the fact of their self configuration ability, they can be deployed urgently barring the need of any infrastructure. Internet Engineering Task Force (IETF) has MANET working crew (WG) that is dedicated for developing IP routing protocols. Routing protocols is one of the difficult and interesting lookup areas. Several routing protocols have been urbanized for MANETS, i.e. AODV, OLSR, DSR etc. Security in Mobile Ad-Hoc Network is the most essential issue for the fundamental functionality of network. The availability of community services, confidentiality and integrity of the facts can be finished via assuring that safety troubles have been met. MANETs regularly suffer from security assaults due to the fact of its

elements like open medium altering its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These elements have modified the warfare subject state of affairs for the MANETs against the safety threats.

The MANETs work except a centralized administration where the nodes speak with each other on the groundwork of mutual trust. This attribute makes MANETs greater inclined to be exploited by way of an attacker inside the network. Wireless links also makes the MANETs more prone to attacks, which make it less complicated for the attacker to go interior the community and get get right of entry to the ongoing conversation [9, 21]. Mobile nodes current inside the range of wireless link can overhear and even take part in the network. MANETs ought to have a secure way for transmission and verbal exchange and this is a quite difficult and necessary trouble as there is growing threats of attack on the Mobile Networks. Security is the cry of the day. In order to supply invulnerable verbal exchange and transmission, the engineers should recognize one-of-a-kind kinds of assaults and their outcomes on the MANETs. Wormhole attack, Black hole attack, Sybil attack, flooding attack, routing desk overflow attack, Denial of Service (DoS), selfish node misbehaving, impersonation attack are variety of assaults that a MANET can suffer from. A MANET is extra open to these kinds of assaults due to the fact communication is primarily based on mutual trust between the nodes, there is no central factor for community management, no authorization facility, vigorously altering topology and restrained resources. The routers in MANETs cross freely, in any direction or speed, and are allowed to organize themselves arbitrarily. Such individuals make such a network ”non-engineered” - the community topology changes dynamically and unpredictably. There is no constant infrastructure, and these consequences in nodes willingly forwarding records to any different node, regularly in a peer-to-peer, multi-hop mode. MANETS have a requirement to vigorously determine routing based on availability or visibility of nodes. MANETs also have nodes whose power storage is very limited. Often, they are battery equipped, with very restricted to no recharging or alternative possible.

Conserving electricity whilst attempting to run ordinary operations is a big issue in the sketch and implementation on MANETs. Another limited resource in MANETs in bandwidth. To cope with the power and bandwidth requirements, MANETs hire grouping techniques, in which some nodes perform precise functions (like forwarding/relaying sensor data), while more powerful contributors function extra resource-intensive things to do (like records aggregation, routing etc). As some nodes die, or are put out of service, different nodes shoulder responsibilities. Thus, often, MANETs are heterogeneous networks, with varying member profiles and a varying rely of members. All of the above features of MANETs pose a serious mission in what is regularly simpler to reap or predict in wired or infrastructure primarily based networks. Guaranteeing facts security and reliability is a serious concern. Thus, the decentralized nature, scalable setup and dynamically altering topology makes adhoc networks perfect for a variety of purposes ranging from front-line zones(military, industrial and natural) to data collection (machinery analysis, biosensing) as investigated in [2]. But the same elements pressure the key challenges in deploying and the use of them: device compatibility, connectivity troubles due to varying site visitors profiles, safety and survivability.

II. RELATED WORK

Due to relatively dynamic nature topology in MANET makes routing manner greater difficult and insecure and consequently nodes are greater prone to compromise and are in particular inclined to denial of provider attack (DoS) assaults launched via [1] malicious nodes or intruders. Hence routing is [2] greater complex and insecure. The wireless nodes are inclined to compromise and inclined to a number of kinds of attacks like DoS (denial of Service), wormhole attack, flooding, green hole attack, black gap attack and egocentric node attack. These all are affect the performance of MANET. Denial of provider (DoS) attacks start via intruders to stop the carrier being used by legitimated users. Route request (RREQ) is one of flooding assault [3] [4] launched by nodes in disbursed manner in such a intention that compromised node can takes gain of the route discovery system and floods the whole network by way of propagating large range of pretend route request (RREQs) for this reason [18] network is jammed main to a denial of service.

Khokhar, R. H., Ngadi, M. A., & Mandala, S. (2008) tackled the importance of security in MANET. According to Deng, H., Li, W., & Agrawal, D. P. (2002) securing of MANET is make positive mutual

authentication of participants nodes, confidentiality and integrity of exchanged data, availability of the network resources, get right of entry to control to the conversation medium and the anonymity. According to Bandyopadhyay, A., Vuppala, S., & Choudhury, P. (2011, February) MANET attacks commonly consists of trying to drop or modify packets, gaining authentication or buying authorization by using 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 some other variant of the DoS is Flooding Attack the Flooding Attack is a denial-of-service assault in which malicious nodes which malicious node sends the useless packets to consume the treasured community resources. Flooding assault is viable in [8][9] all most all on demand routing protocol.

B. Routing desk overflow

C. Impersonation

A node might also perhaps impersonate some other node and send false routing data masqueraded as some other everyday node.

D. Power consumption

E. Information disclosure

In cellular ad hoc networks, packets with facts consisting of reputation of a node, location, non-public or secret keys and passwords, are without difficulty eaves dropped due to the nature of broadcast.

F. Packet modifying

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

G. Selfish Node

Selfish nodes are these which retailer their assets by not taking section in communication.

H. Black hole

It is a kind of egocentric node that simply drops the packets [10] and hence the transmission similarly. A malicious node diverts the vacation spot via sending flawed RREP (route reply) that it has a modern-day route with minimal hop be counted to vacation spot 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 now not ahead them. Gray Hole attack can be act as a sluggish poison in the community side that is the chance of packet loss is undetermined [13] [14].

J. Worm Hole

A worm gap assault is when two or more malicious nodes might also collaborate to encapsulate and change messages between them alongside present data routes. A worm hole displays the route that may also seem first-class to the destination however it constantly tunnels the packet to its malicious companion node. This attack is additionally [15] regarded as tunneling attack.

K. Many techniques has been proposed to remedy the wormhole detection and prevention writer of has review and addresses a technique primarily based on a variant of the counting method in which nodes broadcast group of hashes of the packets acquired out of remaining okay time intervals.

L. Choudhury, P., Nandi, S., Pal, A., & Debnath, N. C. (2012, July) has determined that Ad hoc network and its applied in to topology amongst nodes are extraordinarily dynamic in nature (unstable due to mobility),in such scenarios the routing system is to be more [16] complicated and anxious.

M. Another prospect about wireless operated gadgets or nodes are they are very a good deal prone to compromise. Specifically they are the first preference of goal of attacker for DoS attack.

N. Denial of carrier (DoS) (also called flooding) is two types manage and data flooding. Control flooding is also called RREQ flooding [17] [18] in which excess variety of RREQ is flooded in the adhoc network that prevents other node to get entry to the services. When set of suspicious nodes are generate extra wide variety of RREQ request it is termed as Distributed Denial of Service (DDoS) attack in which a compromised node takes advantage of the route discovery mechanism of on demand routing protocols of MANET and jam (floods) the entire community thru transmitting massive wide

variety of forged RREQs to fictional nodes in the community and leading to a denial of carrier [19] attack.

O. Most of the protection related MANET research is founded in round AODV routing protocols. In this article we are going to evaluate the impact of the flooding assault in DSR on demand routing protocols.

P. Hence Flooding assault has emerge as a primary security challenge in [19] current years. It is the novel research vicinity on account that last three years because none of the present strategies are proposed so a ways detecting and controlling of the have an effect on of flooding in wireless or MANET in realistic aspect.

Q. Everything has two sides, pros and cons. Mobile adhoc gives immediately answer for conversation when requires besides organising infrastructure with wi-fi mobility feature. MANET is a kind of computerized networks which composed of flexible, dynamic, and absolutely self sustaining network entities that can (re)systematize in accordance with the operational, cost-effective, and societal desires of the users and organizations.

R. Although MANET presents quick and fast conversation environment the usage of atomicity (multihop routing), its utility and performance would be spectacularly obstruct in [20] absence of security measure. One of them assault is Denial of Service attack (flooding) launched with the aid of taking the blessings of MANET [22] routing thought (flooding in route discovery) and multihop communication.

S. Although there is a lot of convention safety method used in wired community to realize and prevent DoS attack but the major problem with such method is dynamic nature of MANET because network topology continuously changes.

T. Hence typical methods are inefficient.. Another problem is novelty in attacks (intrusion) hence signature primarily based mechanism does not operate properly in such scenario.

III. PROPOSED WORK

Mobile Ad hoc network (MANET) is a new paradigm in wi-fi revolution, which is a self-configured network of wireless cell nodes. Due to proliferation of miniature yet effective mobile computing devices, it is gaining acceptance and popularity. However, MANET is susceptible to security attacks due to its inherent characteristics such as dynamic topology, lack of a centralized coordinator and open wi-fi channel. In this paper, writer analyzes some safety attacks of MANET and we endorse to identify the assault through the use of an Intrusion Detection System (IDS). The proposed IDS use fuzzy logic to become aware of malicious behavior and pick out the attacks.

Existing Method:

Wahengbam, M., & Marchang, N. (2012, March) has found that “While intrusion detection (IDS) approach will work on top of any routing protocol”. Deng, H., Li, W., & Agrawal, D. P. (2002) had chosen the Ad hoc On-demand Distance Vector (AODV) [6] routing protocol for our 89 experimentation. AODV is layout to grant communication between mobile nodes with minimal manage overhead and minimal route acquisition latency.

Author’s survey

Due to its inherent traits such as dynamically altering topology, susceptible physical safety 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 project to say the least. It is extremely easy for malicious nodes, egocentric nodes, covert channels and eavesdroppers to carry down the entire network. As a result, MANETs are prone to various assaults and threats.

An Intrusion Detection System (IDS) will definitely be a necessary ingredient in any complete protection solution.

The cause at the back of this is that a prevention mechanism -such as securing a routing protocol the use of cryptographic primitives - is now not a foolproof mechanism. However, designing an fantastic Intrusion Detection System (IDS) [4], as nicely as other protection mechanisms, requires a deep appreciation of the risk model and adversaries attack capabilities. Identifying safety attacks is similar in nature to medical diagnosis. Just as quite a few illnesses may share some common signs but with various degree, several safety attacks might also share some common conduct such as shedding of

packets with a various degree. However, a disorder may additionally exhibit some specific characteristic not viewed in other diseases.

Fuzzy logic [1-2] is a computational paradigm that gives a mathematical device for dealing with the uncertainty and the imprecision that is involved in human reasoning, two which is also known as approximate reasoning. The interpretability attribute of fuzzy logic, which is the functionality to express understanding in a linguistic way, makes fuzzy logic-based systems appealing for applications such as clinical prognosis [7]. Our fuzzy logic-based IDS two is primarily based on the two system described in [7], two which is used two to two diagnose diabetics.

Baadache, A., & Belmehdi, A. (2012) proposed a format for an Intrusion Detection System that detects intrusion in a MANET caused by malicious nodes launching special kinds of attacks. With the help of fuzzy logic, we tackle three kinds of routing attacks [5], which showcase packet forwarding misbehavior, viz., Black gap attack, Gray hole assault towards a supply and Gray gap attack in the direction of a destination.

Proposed Method:

Wahengbam, M., & Marchang, N. (2012, March) proposed a fuzzy based totally IDS approach on which he used the concept of threshold to observe 3 sorts of MANET attack using AODV routing protocol-

1. Black Hole
2. Gray Hole
3. Packet Forwarding Misbehavior

Modification required in exiting methods

Following troubles are the core component of the proposed work derived from article [1]

Wahengbam, M., & Marchang, N. (2012, March) solely speaking about three attacks. But there is any other largest assault which will additionally consider for nice plan of the IDs i.e. Selfish Node Attack,

1. Authors adopt the thought of fuzzy logic that need to be enhanced, due to the fact false fee will amplify if threshold price not suitable decide. We will undertake the thinking of Machine Learning strategy to plan full IDS machine for the MANET. For this we will use greater SVM machine idea distributives for each node.
2. Routing protocol chosen by using the writer is appropriate however solely AODV alone is no longer applied two two everywhere. So we will think about the different routing protocols as well, like OLSR and DSDV for better optimization.
3. Anomaly detection is the high-quality way to detect other unknown (new) kinds of attack. Our proposed work will undertake the concept of behavioral anomaly detection to format better IDS functionality system.
4. It is found that NS-2 patches are no longer stable they have bugs which will be incompatible for the preceding and subsequent future version. So that for higher assessment we will use NS-3.18 which secure and accurate with better test mattress option for the network related research and techniques especially in wi-fi scenario.

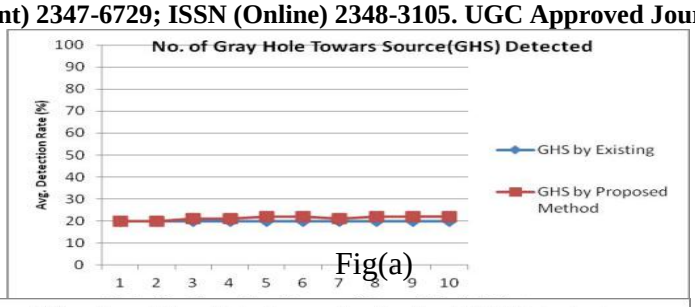
IV. SIMULATION RESULTS

The NS three Introduction: ns (from community simulator) is a identify for sequence of discrete match community simulators, in particular ns-1, ns-2 and ns-3. All of them are discrete-event community simulator, specially used in lookup and teaching. Ns-3 is free software, publicly handy below the GNU GPLv2 license for research, development, and use.

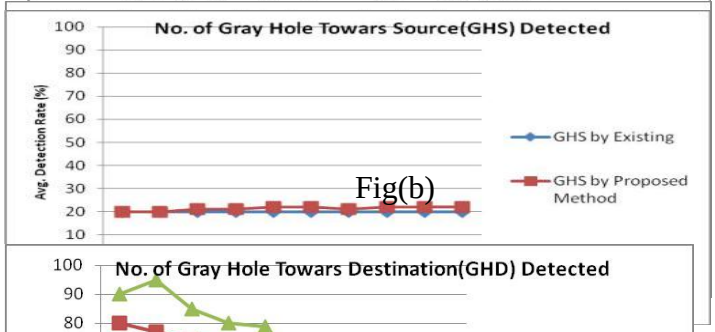
The aim of the ns-3 mission is to create an open simulation environment for networking lookup that will be preferred internal the lookup community:

- It ought to be aligned with the simulation needs of cutting-edge networking research.
- It motivates community contribution, peer review, and validation of the software.

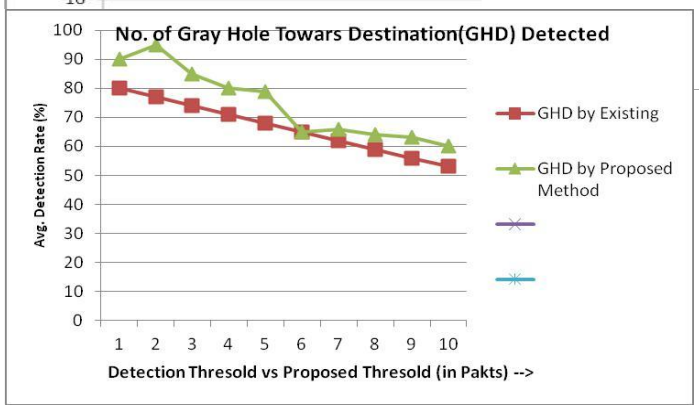
Since the manner of advent of a network simulator that includes a ample variety of amazing validated, tested and actively maintained fashions requires a lot of work, ns-3 task spreads this workload over a massive neighborhood of users and developers.



Fig(a)



Fig(b)



Fig(c)

V. CONCLUSION

Security in MANET is the today's need of fine and invulnerable communication. IDS in MANET has want proper interest to stop unauthorized attack such as selfish node, black hole and grey gap attack. In this article we have survey the authors proposed the solution for the black hole (BH) and gray gap of both type towards supply and destination. Both the assaults are most frequent and harmful in MANT scenario. Author has adopted the thinking of threshold mechanism making use of on packet drop metrics to calculate maliciousness regionally (by each node) the use of fuzzy logic. Author has reflect on consideration on solely metrics for its comparison i.e. packet drop ratio. In this article we have proposed a more more suitable approach to become aware of intrusion by integrating extra metrics like packet delivery ratio, routing overhead and author's packet drop ratio to calculate the suspiciousness of the node with the help of desktop gaining knowledge of method to classify the nodes whether they are authenticated or intruders. Proposed mechanism has been implemented on NS-3.18 on AODV routing protocols and computing device learning tool. Obtained consequences are better than present method with ease of simplicity and accuracy.

VI. REFERENCES

[1] Wahengbam, M., & Marchang, N. (2012, March). Intrusion detection in manet using fuzzy logic. In Emerging trends and applications in computer science (NCETACS), 2012 3rd national conference on (pp. 189-192). IEEE.

[2] Choudhury, P., Nandi, S., Pal, A., & Debnath, N. C. (2012, July). Mitigating route request flooding attack in MANET using node reputation. In Industrial informatics (INDIN), 2012 10th IEEE international conference on (pp. 1010-1015). IEEE.

[3] Kannhavong, B., Nakayama, H., Nemoto, Y., Kato, N., & Jamalipour, A. (2007). A survey of routing attacks in mobile ad hoc networks. IEEE Wireless communications, 14(5).

[4] Khokhar, R. H., Ngadi, M. A., & Mandala, S. (2008). A review of current routing attacks in mobile ad hoc networks. International Journal of Computer Science and Security, 2(3), 18-29.

[5] Baadache, A., & Belmehdi, A. (2012). Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks. Journal of Network and Computer Applications, 35(3), 1130-1139.

[6] Deng, H., Li, W., & Agrawal, D. P. (2002). Routing security in wireless ad hoc networks. IEEE Communications magazine, 40(10), 70-75.

[7] Bandyopadhyay, A., Vuppala, S., & Choudhury, P. (2011, February). A simulation analysis of flooding attack in MANET using NS-3. In Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on (pp. 1-5). IEEE.

[8] Vani, A., & Rao, D. S. (2011). Providing of secure routing against attacks in manets. International Journal of Computer Applications (0975–8887) Volume.

[9] KarpagaBrinda R, R. (2012). Detection and Removal of Co-Operative Black HoleBlack Hole Attack in Manet. International Journal of Computer Applications, 43(11), 5-9.

[10] Madhusudhananagakumar, K. S., & Aghila, G. (2011). A survey on black hole attacks on aodv protocol in manet. International Journal of Computer Applications (0975–8887) Volume, 23-30.

[11] Vishnu, K., & Paul, A. J. (2010). Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks. International Journal of Computer Applications, 1(22), 38-42.

[12] Chandure, O. V., & Gaikwad, V. T. (2012). Detection & prevention of gray hole attack in mobile ad-hoc network using aodv routing protocol. International Journal of Computer Applications (0975–8887) Volume.

[13] Singh, J., Singh, A., & Shree, R. (2011). An assessment of frequently adopted unsecure patterns in mobile ad hoc network: Requirement and security management perspective. International Journal of Computer Applications (0975–8887), 24(9).

[14] Kumar, M., Bhushan, A., & Kumar, A. (2012). A study of wireless ad-hoc network attack and routing protocol attack. International Journal of Advanced Research in Computer Science and Software Engineering ISSN, 2277.

[15] Pervaiz, M. O., Cardei, M., & Wu, J. (2010). Routing security in ad hoc wireless networks. In Network security (pp. 117-142). Springer, Boston, MA.

[16] Kannhavong, B., Nakayama, H., Nemoto, Y., Kato, N., & Jamalipour, A. (2007). A survey of routing attacks in mobile ad hoc networks. IEEE Wireless communications, 14(5).

[17] Khokhar, R. H., Ngadi, M. A., & Mandala, S. (2008). A review of current routing attacks in mobile ad hoc networks. International Journal of Computer Science and Security, 2(3), 18-29.

[18] Banerjee, A., Vuppala, S., Choudhury, P., & Das, S. (2011, June). Survey of Flooding Attack Remedies in MANET. In Proc. of the International Conference on Communication and Broadband Networking (ICCBN 2011), June 2011.

[19] Zhang, Z., Naït-Abdesselam, F., Ho, P. H., & Kadobayashi, Y. (2011). Toward cost-sensitive self-optimizing anomaly detection and response in autonomic networks. computers & security, 30(6-7), 525-537.

[20] Alikhany, M., & Abadi, M. (2011, February). A dynamic clustering-based approach for anomaly detection in AODV-based MANETs. In Computer Networks and Distributed Systems (CNDS), 2011 International Symposium on (pp. 67-72). IEEE.