iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** X **Month of publication:** October 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Intrusion Detection in Mobile Ad Hoc Network

Rashmi
M.Tech in Computer Science, Shobhit University Meerut

***Abstract*—MANETs are prone to various active and passive security attacks and intrusions.Cryptography and authentication systems are not well sufficient for MANETs. It is required that MANETs should have the ability to detect any attack or intrusion as it comes into thenetwork.Various IDS systems are proposed to detect such intrusions and security attacks but these must be modified as these are insufficient,especially for WAN(wireless ad-hoc networks) due to the differences in WANs characteristics. In this paper it is proposed to modify IDS for a special type of DOS(Denial of Service) for a neighbouring node that is deprived of its fair usage of transmission channel.Results comparisons are also been shown.**
***Keywords*—MANET,IDS(Intrusion Detection System),Threshold,DOS(Denial of Service),Attacks**

I. INTRODUCTION

In a mobile ad hoc network (MANET), a collection of mobile hosts with wireless network interfaces form a temporary network without the aid of any fixed infrastructure or centralized administration Intrusion detection can be defined as a process of monitoring activities in a system, which can be a computer or network system. The mechanism by which this is achieved is called an intrusion detection system (IDS).

A. ATTACKS

There are both passive and active attacks in MANETs. For passive attacks, packets containing secret information might be eavesdropped, which violates confidentiality. Active attacks, including injecting packets to invalid destinations into the network, deleting packets, modifying the contents of packets

B. Security Attribute

Security is the combination of processes, procedures, and systems used to ensure confidentiality, authentication, integrity, availability, access control, and non-repudiation

II. ARCHITECTURES AND TECHNIQUES FOR IDS IN MANETS

The MANETs can be configured to either of two network infrastructures (i) flat or (ii) multi-layer, depending on the applications. In a flat network infrastructure, all nodes are considered equal, thus it may be suitable for applications such as virtual classrooms or conferences. On the contrary, some nodes are considered different in the multi-layered network infrastructure.

A. Distributed And Cooperative Ids

Each node communicates with its neighboring nodes through the IDS.IDS from one node is transferred to its neighboring nodes to get knowledge of the nodes. Distributed and cooperative as shown in figure.

B. Hierarchical IDS

Hierarchical IDS architectures extend the distributed and cooperative IDS architectures to multi-layered network infrastructures where the network is divided into clustersShows a figure Hierarchical cluster structure, black nodes represent a clusterhead, gray nodes represent nodes responsible for inter-cluster communication and white nodes are the other nodes with in a cluster.

There are several proposed techniques and protocols to detect such misbehavior in order to avoid those nodes.

III. PROPOSED INTRUSION DETECTION SCHEME FOR MOBILE ADHOC NETWORKS

Watch dog and Path-rater, to be added on top of the standard routing protocol in ad-hoc networks. Dynamic Source Routing protocol (DSR) is chosen for the discussion to explain the concepts of Watchdog and Path-rater.The watchdog method detects misbehaving nodes.. A path-rater then helps to find the routes that do not contain those misbehaving nodes. In DSR, the routing information is defined at the source node. This routing information is passed together with the message through intermediate nodes until it reaches the destination.

We aim to detect a particular type of Denial of Service attack, which victimizes neighboring nodes by unfair use of the shared wireless link. A node can prevent other nodes in its neighborhood from getting fair share of the transmission channel in a number of ways. This misbehavior can be considered as DoS (Denial of Service) attack against the competing neighbors in a contention-based network since the competing neighbors are deprived of their fair share of the transmission channel. The possible methods for this type of attack are as follows:

A. Not complying with the MAC protocol:Contention based MAC (Medium Access Control) protocols, such as IEEE 802.11, use RTS and CTS to notify the immediate neighbors of the transmitters and receivers that a transmission of data will take place for a period as specified in RTS/CTS packets. RTS/CTS and the backoff mechanism aim to minimize collisions among competing neighbors and try to ensure that all the competing neighbors can get some share of the common channel.

1) However a node can generate RTS/CTS at an unacceptable rate by ignoring the backoff mechanism so that competing neighbors cannot get an adequate share of the transmission channel. This can cause the packets waiting at the output queues of the competing neighbors to wait for too long until they time out and get removed.

2) Both RTS and CTS contain fields that notify neighboring nodes for how long a channel will be occupied for successful transmission of the associated data packets. If the indicated duration (Ti) is more than the actual duration (Ta) taken for successful transmissions, the transmission channel will remain occupied for an additional period, Ti - Ta. The competing neighbors may not be aware of this additional hidden period. As a consequence neighbors will be debarred from using the channel for this additional period

3) .If the indicated duration (Ti) is less than the actual duration (Ta) taken for successful transmissions, then neighbors trying to access the channel are likely to face unexpected collisions, thus neighbors increase their backoff intervals and hence may not get their share of the channel.

B. Jamming the transmission channel with garbage:Garbage can consist of packets of unknown formats, MAC layer packets violating the proper sequence of a transaction (e.g. sending a data packet without exchanging RTS and CTS) or simply random bits used as static noise by misbehaving nodes. Garbage data may result in too many collisions, may consume a significant part of the available channel capacity or both. Consequently legitimate neighbors may not be able to access the channel properly when needed.

C. Not complying with the bandwidth reservation scheme:Nodes in a multi-hop wireless network can reserve bandwidth, i.e. a portion of the transmission channel capacity, along its route before initiating a flow. If there is not enough bandwidth, new flows should not be admitted so that existing flows are not choked. A misbehaving node may not abide by this rule and try to push out packets when there is not enough bandwidth left. As a result legitimate nodes may not get fair share of the transmission channel.

IV. DETECTING ATTACK AND IDENTIFICATION OF ATTACKER

We make the following assumption to detect the above attack. Traffic flows allocate bandwidth (i.e. link capacity) at each routing node before they can begin their actual transmissions. If there is not enough bandwidth, additional flows are not admitted. This enables existing flows to achieve their desired QoS.

Let us assume that for each period T, a node knows that p% of the available link capacity has been allocated to it by its neighboring nodes where $p \leq L$ where L is the total link capacity. L should be less than 100% since no system can work at 100% capacity. We have set it to 90%. Now for each period T, every node measures the percentage of link capacity r% being used by each of the

neighboring nodes for the admitted flows and u% being utilized due to flows that did not reserve bandwidth. It also measures the percentage of link capacity s% being wasted due to collisions (intentional by attacker or unintentional due to IEEE 802.11 protocol weakness) and garbage data sent by attacker node. If $(\sum(r+u) + s) \geq (L - p)$, then a node assumes that a neighbor or a group of neighbors are accessing the channel unfairly. Since r and u can be measured easily by every node by listening to RTS packets of other nodes for every time interval T, so it becomes possible to identify the unfair excessive use by a node if $(r + u) > p$. Every neighboring node increases its non-negative misbehavior counter MC [excessive use, N] for suspicious node N each time such an attack is detected and decrements it if there is no such misbehavior. If MC [excessive use, N] reaches a threshold, then a node declares its neighborhood N as misbehaving.

Sometimes a neighbor node may not send packets at a constant bit rate and thus may not utilize the whole part of link capacity allocated to its admitted flow. Hence r can be less than p. Therefore, $r < p$ does not mean that neighbors are not getting fair share of the channel. However, $r < p$ can also be true if a neighbor does not get fair share of the channel.

V. SIMULATION

GloMoSim (version 2.02) used for simulating various layers and wireless media. 70 nodes are placed on a 3000 meter by 3000 meter flat terrain where they are separated by at most 240 meters, use the same transmission power with a transmission range of maximum 240 meters, share the same frequency channel and use IEEE 802.11 in the link layer. The physical layer modulates/demodulates signals using OFDM (Orthogonal Frequency Division Multiplexing) with a transmission rate of 54 Mbps and uses a single network card with a single omnidirectional antenna. The routing has been done using DSR. For each simulation run, we have randomly selected twelve pairs of source and destination where each node pair is separated at least by four intermediate nodes and creates a 1.46 Mbps UDP type CBR (Constant Bit Rate) flow at random time. Once a flow is initiated, it is executed until the end of each simulation run. Simulation time for each run was set to 180 seconds. IT have logged the values of two performance metrics, throughput and delay every 2 seconds. The source and destination node pairs were evenly distributed over the whole network in order to reduce the effect of network congestion on the network performance for overlapping sessions so that only the misbehavior related effects become prominent. For each type of attack we have randomly selected four misbehaving nodes where each of them can initiate misbehavior at any time but continues to misbehave till the end of the simulation run. Each type of attack was performed in ten simulation runs to obtain average values of the associated performance metrics.

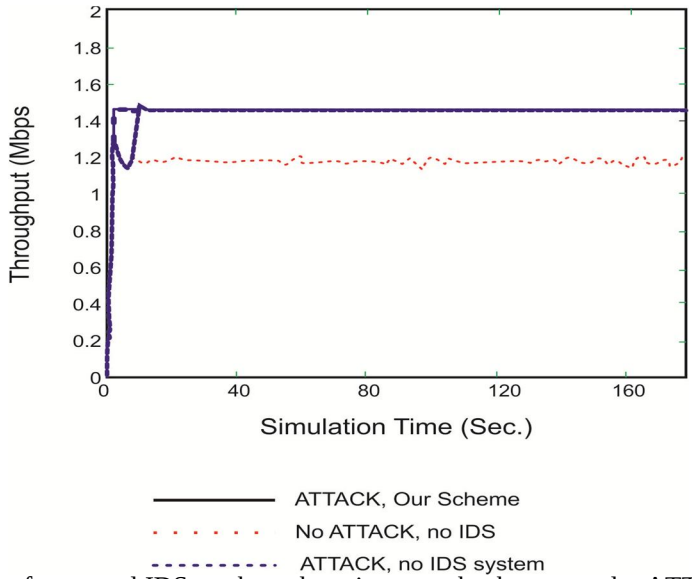


Figure 1: Effect of proposed IDS on throughput in networks that are under ATTACK but do not have any intrusion detection

The threshold for the misbehavior counts, i.e. MC's, of attack was set to four. Initiating a flow at the misbehaving node without reserving bandwidth where the channel capacity required for the flow was more than the available channel capacity created ATTACK. Figures 1 and 2 show the effectiveness of our scheme thorough two performance metrics. The sudden improvements in network performance indicate that our scheme is able to detect various attacks and can take necessary actions, i.e. find an alternate route, to achieve the desired network performance.

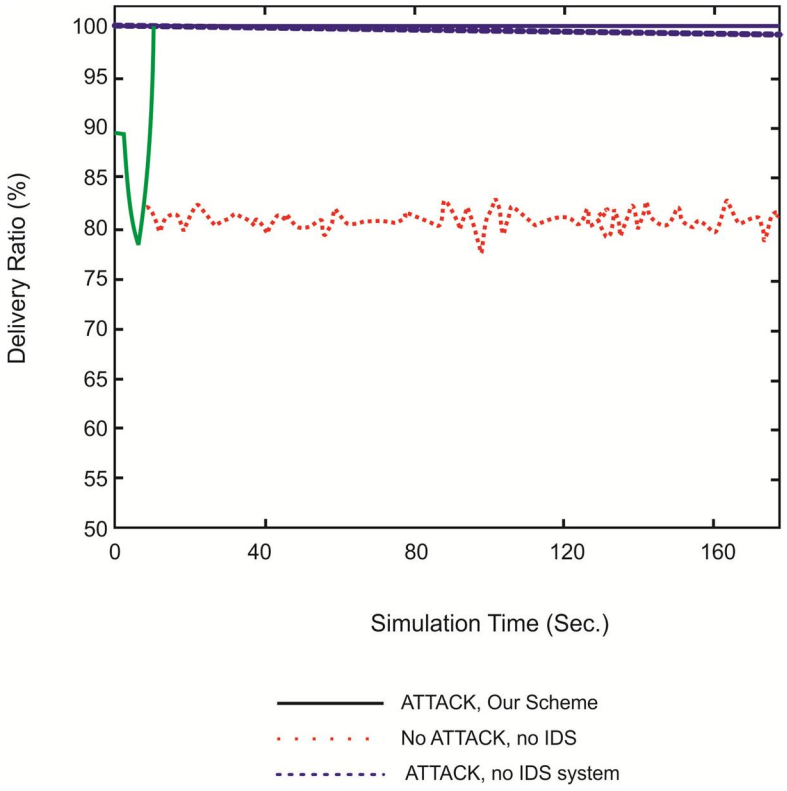


Figure 2: Effect of perposed IDS on Delivery Ratio in networks that are under ATTACK but do not have any intrusion detection *system.*

The desired network performance has been shown by "no Attack, no IDS" line in each graph which was obtained by performing the simulations without any attack.

VI. CONCLUSIONS

In This Paper the intrusion detection system has been proposed. The proposed IDS does rely on overhearing packet transmissions of neighboring nodes which makes it an effective system in networks where nodes use different transmission power and directional antennas for different neighbors. The proposed IDS select various thresholds dynamically. . Moreover, a fully functional intrusion response system can be developed that would cater to all types of DoS attacks at routing layer also.

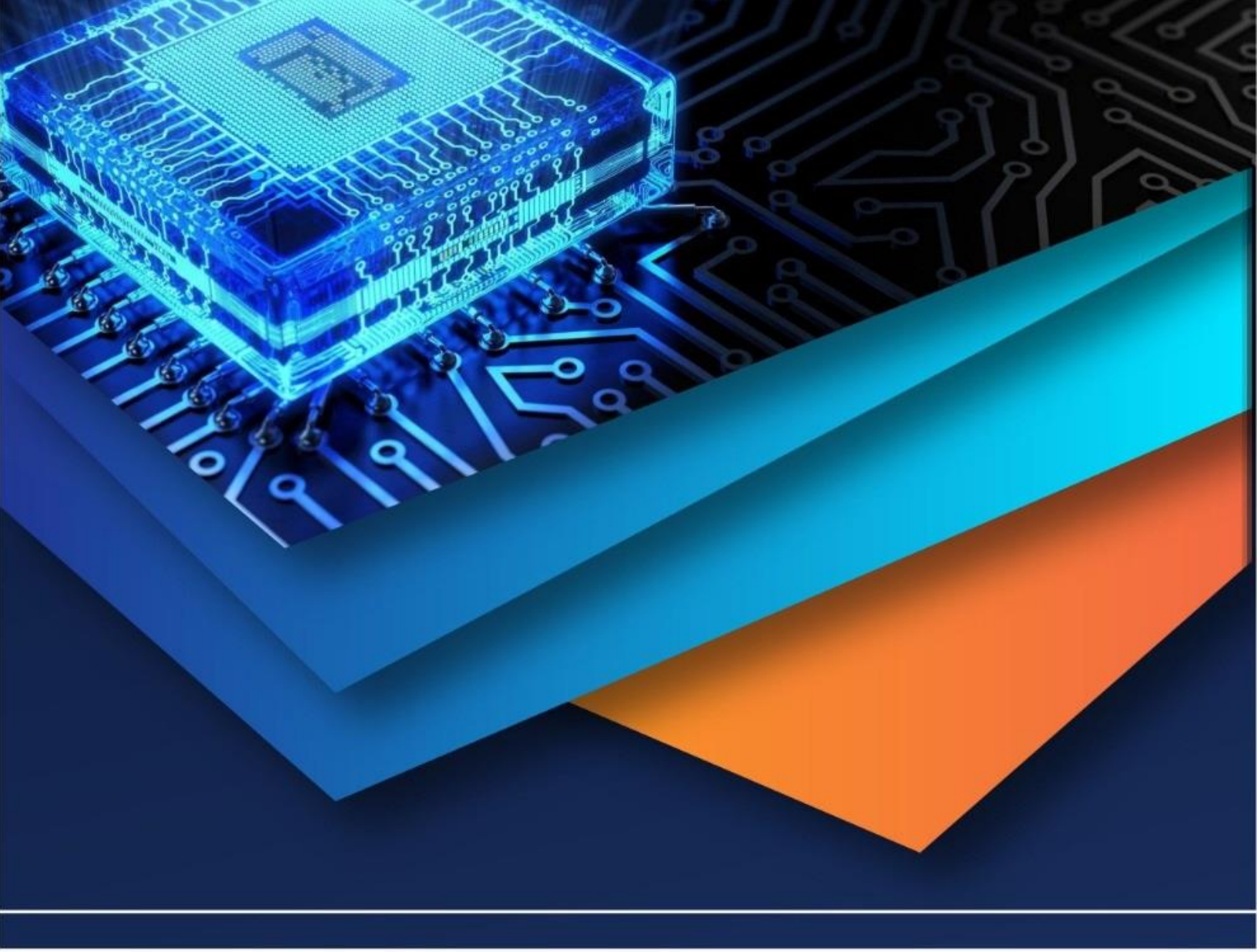
VII. ACKNOWLEDGMENT

I am highly indebted and graceful to **Mr. Vijay Maheshwari,** Assistant Professor, Department of Computer Science and Information Technology, Faculty of Engineering, Shobhit University, Meerut, for their strict supervision, constant encouragement, inspiration and guidance which ensure the worthiness of my thesis work. Working under him was an enriching experience.

My sincere regards are to Hon'ble Vice-Chancellor and Registrar for their valuable leadership to create high academic environment in the University and Dr. NirajSinghal, M.Tech-Coordinator for providing me the opportunity and facilities to complete my work.

REFERENCES

[1] TiranuchAnantvalee, Jie Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks" Wireless/Mobile Network Security Journal, pp. 170 – 196, 2006 Springer
[2] Y. Zhang, W. Lee, and Y. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks," ACM/Kluwer Wireless Networks Journal (ACM WINET), Vol. 9, No. 5, September 2003
[3] M. Wegmuller, J. P. voTapan P. Gondaliya, Maninder Singh, "intrusion detection System for Attack Prevention in Mobile Ad-hoc Network", International Journal of Advanced Research in Computer Science and SoftwareEngineering Volume 3, Issue 4, April 2011.
[4] Barani, F., &Abadi, M.I. BeeID: intrusion detection inAODV-based MANETs using artificial beecolony and negative selection algorithms, The ISC International Journal of Information Security, 1,4, 2012.
[5] P. Sil, R. Chaki, N. Chaki; "HIDS: Honesty-rate based collaborative Intrusion Detection System forMobile Ad-Hoc Networks", Proc. of 7th IEEE International Conference on Computer InformationSystems and Industrial Management Applications (CISIM), 2008
[6] Ponomarchuk, Yulia and Seo, Dae-Wha, "Intrusion Detection Based On Traffic Analysis in Wireless Sensor Networks" IEEE 2010.
[7] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion Detection in Wireless Ad Hoc Networks," IEEE Wireless Communications, Vol. 11, Issue 1, pp. 48-60, February 2004.
[8] P. Albers, O. Camp, J. Percher, B. Jouga, L. M, and R. Puttini, "Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches," Proceedings of the 1st International Workshop on Wireless Information Systems (WIS-2002), pp. 1-12, April 2002.
[9] O. Kachirski and R. Guha , "Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks," Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03), p. 57.1, January 2003.
[10] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom'00), pp. 255-265, August 2000.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY