

Remapping Attack Detection and Prevention for Reliable data service in MANET

Ishwarlal Rathod

Asst. Professor

Symbiosis University of Applied Sciences Indore (M.P)

ishwarlal.rathod@suas.ac.in; en21el601003@medicaps.ac.in

Ankit Saxena

Assoc. Professor

Medi-caps University Indore (M.P)

Ankit.saxena@medicaps.ac.in

Abstract. Mobile ad hoc Network is a promising technology in recent years. The number of nodes are forming dynamic link in between sender and receiver. The Mobile ad hoc Network (MANET) are operating in absence of centralized administration and because of that attackers are simply changed or acting malicious activities in network. One in all the most important challenge in wireless mobile ad-hoc sensor networks nowadays is protection. In this title we tend to plan a completely unique security scheme for Remapping Attack. This type of attacks is amendment the priority of communication and acting misbehavior through flooding of huge quantity of reserve packets in communication network. The attacker node is provides the primary priority itself for information sending and remainder of the nodes priority is come back when attacker. The proposed results of assaulter malicious activities are consumed link bandwidth and additionally actual data delivery in network is affected. The aim of this research is to measure the malicious performance of Remapping attack in MANET and identifies the node/s that are affected the routing performance. The proposed security theme are check the priority order of each sender node in network that require to communicate and solely the offender is one altogether the node that flooded the reserve packets in network and in addition the assaulter node is not the sender or receiver. The proposed security scheme against remapping are block the activity of offender. The performance of network is measured on the basis of performance metrics like as network throughput, PDF and routing overhead, attacker node identification.

Keywords: MANET, Security, Remapping Attack, flooding, Routing.

1 Introduction

Mobile Mobile Ad-hoc Networks (MANETs) has become one in each of the foremost prevailing areas of research at intervals the recent years as results of the challenges it cause to the connected protocols. MANET is that the new rising technology that allows users to communicate without physical infrastructure however their geographical location, that's why it's generally aforesaid as an infrastructure less network. The enhance low price, light-weight and energy primarily based devices builds MANET a fastest growing network. MANET is self-organizing and accommodative. Devices in MANET is sensor nodes that must to be able to observe the presence of various devices and perform necessary recognized to facilitate communication and sharing of data and repair. MANET permits the devices to need care of connections to the network still as merely adding and removing devices to and from the network [4]. as a result of nodal quality, the configuration may change quickly and erratically over time. The network is localized, where network organization and message delivery have to be compelled to be compelled to be dead by the nodes themselves. Message routing is in addition a drawback throughout a modify atmosphere where the topology fluctuate. Whereas the shortest path from a provide to a

destination supported a given price perform throughout a static network is often the optimum route, this concept is hard to extend in painter [4-6]. The set of applications for MANET is miscellaneous, ranging from large-scale, mobile, very dynamic networks, to small, static networks that are unnatural by power sources. As Wireless networks became extra and extra trendy within the past few decades, significantly within the 1990's once they're being tailored to vary quality and wireless devices became fashionable. As a results of the standard of mobile devices (MDs) and wireless networks significantly enlarged over the past years, wireless unplanned networks has presently become one in each of the foremost spirited and active fields of communication and networking analysis. As there are many collaborating future applications of mobile unplanned networks (MANET), there are still some essential challenges and open problems to be resolved.

The offenders in network endlessly deliver the massive quantity of packets in network at whole entirely totally different live and besides modification the priority of communication of senders this kind of behavior of offender unit of measurement referred to as Traffic Remapping Attack (TRA). This attack are consumes the complete link capacity of network by that nodes don't seem to be deliver the any info in network. Throughout this paper the authors are to develop a replacement profile based theme for shielding network from attack [1-3].

2 Related Work

Jerzy Konorski and SzymonSzott,[1] "Discouraging Traffic Remapping Attacks in local Ad hoc Networks" this research work is provides the security scheme of discouragement theme supported the threat of TRA detection and human action. The theme doesn't suppose station identities or a real third party, nor will it might like change of state with the MAC protocol. These authors are analyze an arising non-cooperative TRA scheme and see that at a lower place bound realistic assumptions it solely incentivizes TRAs if they harmless to entirely totally different stations otherwise the egotistical stations return to mind to search out out those TRAs square measure harmful.

Bing Wu, Jianmin Chen, Jie Wu, MihaelaCardei [4] "A Survey on Attacks and Countermeasures in Mobile Ad hoc Networks" in this paper proposed countermeasures are choices or functions that produce or eliminate security vulnerabilities and attacks. First, they offer an outline of attacks reliable with the protocols stacks, and to security attributes and mechanisms. Then they proposed security approaches following the order of the superimposed protocol stacks. They are in addition suggests an outline of MANET Intrusion Detection Systems (IDS), that are reactive approaches to frustrate attacks and used as a second line of defense.

Abhay Kumar Rai et. al. has been planned a title [5] "Different varieties of Attacks on Integrated MANET-Internet Communication" during this work they focus on varied varieties of attacks on integrated MANET-Internet communication. They take into consideration commonest varieties of attacks on mobile unintentional networks and on access purpose through that MANET is connected to the online. Specifically, they study but varied attacks influence the performance of the network and choose the safety issues that haven't solved until currently.

K.P.Manikandanet. al. has planned a paper on title [6] "Survey on Attacks and Defense Metrics of Routing Mechanism in Mobile ad hoc Networks" during this title we tend to tend identified the existent security threats an ad hoc network faces, the safety services needed to be achieved and together the countermeasures for attacks in routing protocols. To accomplish our goal, they have done literature survey in gathering info associated with varied varieties of attacks and solutions. Finally, they have well-known the challenges and projected solutions to beat them. In our survey, we tend to tend to specialize at intervals the findings and connected works from that to supply secure protocols for MANET. However, in short, we tend to are ready to say that the complete security resolution desires the hindrance, detection and reaction mechanisms applied in MANET.

Himadri Nath Saha , Dr. Debika Bhattacharyya , Dr. P. K.Banerjee[7] "Study of various Attacks In MANET With Its Detection & Mitigation Schemes" This title additionally classifies many common attacks against the unintentional networks routing protocols primarily based upon the techniques that might be employed by attackers to take advantage of routing messages.

Shikha faith [8] "Security Threats in MANETs: A Review" during this title they discuss MANET are the special networks shaped for specific applications. Operative throughout MANET permits all wireless devices at

intervals vary of every entirely totally different to search out and communicate throughout a peer-to-peer fashion whereas not involving central access points. Several routing protocols like AODV, DSR etc are proposed for these networks to hunt out an end to end path between the nodes. These routing protocols are in danger of attacks by the malicious nodes. There's a demand to look at and stop these attacks throughout a timely manner before destruction of network services.

SupriyaTayal ,Vinti Gupta[9] "A Survey of Attacks on MANET Routing Protocols" in this title they have got tried to represent an outline of AODV, the attainable attacks on MANET and a few security mechanism to those attacks.

Sk.RahimaSulthana, D.Srujan Chandra Reddy,T.Bharath Manohar [10] "An Efficient Mechanism of Handling MANET Routing Attacks victimization Risk Aware Mitigation with Distributed Node Control" in this work these authors are proposed debate a risk- aware response mechanism to consistently modify the famous routing attacks. This risk aware approach relies on an extended Dempster-Shafer mathematical theory of proof introducing a notion of importance factors. additionally, their experiments demonstrate the effectiveness of our approach with the thought of the various performance metrics.

Sevil Sen., John A. Clark [11] "Evolutionary Computation Techniques for Intrusion Detection in Mobile Ad hoc Networks" in this paper authors are proposed to explore the use of evolutionary computation techniques, considerably genetic programming and grammatical evolution, to evolve intrusion detection programs for such tough environments. Aware of the particular importance of power potency we tend to analyze the power consumption of evolved programs and use a multi-objective evolutionary algorithmic rule to induce best trade-offs between intrusion detection ability and power consumption.

Gagandeep, Aashima, Pawan Kumar [12]"Analysis of various Security Attacks in MANETs on Protocol Stack A-Review. Focus is on routing and security issues associated with MANET that are required therefore on offer secure communication. On the basis of the character of attack interaction, the attacks against MANET also are classified into active and passive attacks. Attackers against a network are typically classified into 2 groups like insider and outsider. Whereas are outsider offender isn't a legitimate user of the network, an executive director offender is a licensed node and a district of the routing mechanism on MANET.

Er.KiranNarang, Sonal [13] " A Study of various Attacks in MANET and Discussion concerning Solutions of Blackhole Attack on AODV Protocol" this title represent , a review of varied types of attacks and existing solutions of blackhole attack and their demerits. Therefore MANET is accessible to every legitimate network users and malicious attackers. There are many routing attacks caused due to lack of security .The one in every of best suited protocol is AODV for MANET and it's liable to part attack by malicious nodes. It's virtually just like the part at intervals the universe at intervals that things disappear. The part attack is that where a malicious node advertises itself as a result of it's the optimum route to the destination by causing RREP message with highest sequence selection and minimum hop count.

3 Proposed Work

The Traffic remapping attack is similar as Denial of service attack. Denial of Service (or DoS) attacks are a kind of attacks against computers connected to the Internet and spread of flood the unwanted junk message in the network. The traffic remapping attack similarly generate the unwanted message in huge amount and sense the ideal terminal and sends junk of message in continues manner, that attack consume the network security as well as change the data priority. So here we design algorithm for detection and protection of traffic remapping attack mobile ad-hoc network communication, very first we initialize all variable and check the behaviour of remapping attacker, if any node send undefined type packet in very higher rate means lunching the remapping attack that change the priority of communication in network and damage the protocols of network. The traffic remapping attack detected by analyzing the traffic behaviour and its data sending rate based methodology. After that detection of attack we apply protection scheme so we create protector node p that node watch neighbour node activity as well as their vulnerabilities and retrieve the information about attack and rate of data exchanging between attacker and captured by attacker node that behaviour for useful for protector p node for protection. But

initially p node send the rate control message to the attacker node and if attacker node will not control there rate so p node block the particular traffic remapping attacker node and protect the whole mobile ad-hocnetwork.

3.1 ProposedAlgorithm

In our mobile sensor communication all node play a important role because all are work collaborative form or dependent base route, that provide one measure issue is security so here we design algorithm for detection and protection of traffic remapping attack under sensor communication, very first we initialize all variable and check the behaviour of traffic remapping attack, if any node send undefined type packet in very higher rate means lunningg the remapping attack that change the priority of communication in network, but that type of attack measured through historic data analysis base technique and detect the attacker node, after that we apply protection scheme so we create protector node p that node watch whole neighbour node activity as well as vulnerable node and retrieve the information about attack and rate of data exchanging between attacker and vulnerable node, and send the rate control message to the attacker node.

That historic analysis base detection and future time real time protection provide strength to the communication network in the form of security issue.

Input parameter

Step 1: Sensor Nodes: N; MAC layer: 802.11

Routing Protocol: AODV Attack Type: Remapping

Security Mechanism: PPS (Profile based Protection Scheme) Inter Arrival Time = IAT (priority based)

//Attacker launches remapping attack

Attacker-node (capture vulnerable node information && send = abnormal packet && rate = $2^{20} \times 0.1s$)

If (vulnerable receiver data)

{

Infected;

Call Remapping attack Module;

}

Step generate trace file for further analysis Step analysis trace for detection

If (data type == Remapping a&& rate >= normal)

{

Packet is unwanted remapping attack type; Find infection ratio;

Priority of attacker is high

}

Step: Call protector PPS

While (PPS-Check susceptible node && total data receives && rate && sender)

{

If (rate >= normal && packet =Remapping)

{

Send rate control message at different Inter Arrival Time If (control rate = true)

{

Cannot block;

Proper provides priority to senders;

}

Else {block the sender node ;}

} }

4 Outcome of Our Proposed Work

In this section describe our result outcomes in thirty mobile node cases and conclude our results.

A. Overall Analysis

The overall performance of network is mentioned in table 1.2. In this analysis the priority based scenarios of normal routing performance are represents by S1, S2 and S3. Also include the scenario of remapping attack and security against attack. The scenario represent the individual performance of both transport layer protocol like TCP and UDP and identified that the security scheme is provides secure communication in dynamic network

Table 1. Summarized Performance Analysis

Parameter	Overall Summery S1	Overall Summery S2	Overall Summery S3	Overall Summery Secure	Overall Summery Attack
TCP SEND	3326	4350	4828	2733	1260
UDP SEND	4979	4979	4979	4979	4979
TCP RECV	3309	4310	4809	2678	1221
UDP RECV	3155	4797	3844	4978	724
ROUTINGPKTS	1789	860	1053	561	210268
TCP-PDF	99.49	99.08	99.61	97.99	96.9
UDP-PDF	63.37	96.34	77.2	99.98	14.54
Average e-e delay(ms)	1017.3	396.06	426.18	533.58	1470.25
NRL	0.28	0.09	0.12	0.07	108.11
Attack	0	0	0	0	360104
Total Drop	1841	222	1154	56	4294

B. Attacker Node Analysis

The attacker is always performing misbehaviour in network and the routing performance of network is completely degrades due to less packets receiving and heavy packet loss. The table 1.3 is represents the attacker nodes packet capturing analysis. In this table the six nodes are identified in network that performing malicious activities in network. The node 1 is captures highest number of packets and node 9 is lowest.

Table 2. Attacker Analysis

Attacker Node	Packet Capture	Percentage of Infection
1	151084	57.18
5	55378	20.96
7	58726	22.23
9	58	0.02
15	52420	19.84
22	42438	16.06

C. PDR Analysis

In following graph (Figure 1), we measure the Packet Delivery Ratio performance at the time of Routing, Attack and after the proposed security mechanism. The proposed mechanism improves the performance and provides efficient packet delivery in the network. The graph showing simulation time (in Sec.) and Percentage of data receiving, during difference scenarios. The Result concludes that proposed security mechanism defends the attacker node from data transmission or participation in communication, meanwhile our data transmission ratio is improved.

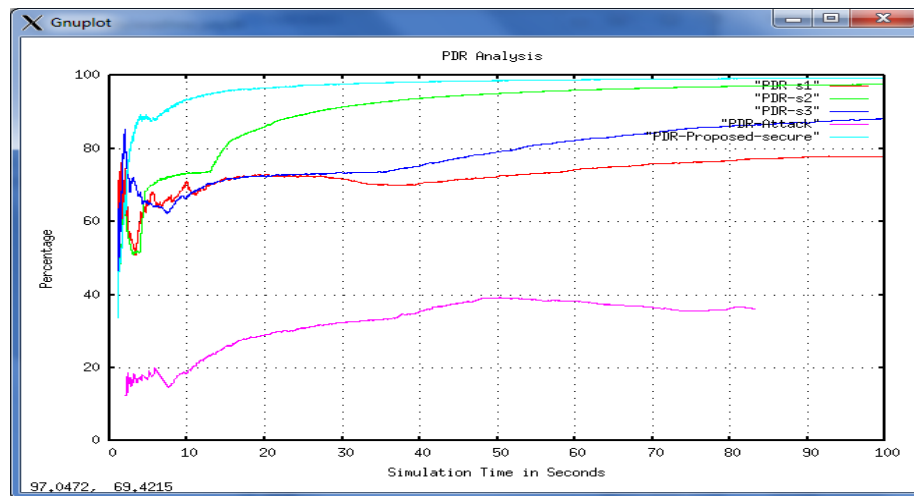


Fig. 1. PDR Performance Analysis

D. Throughput Analysis

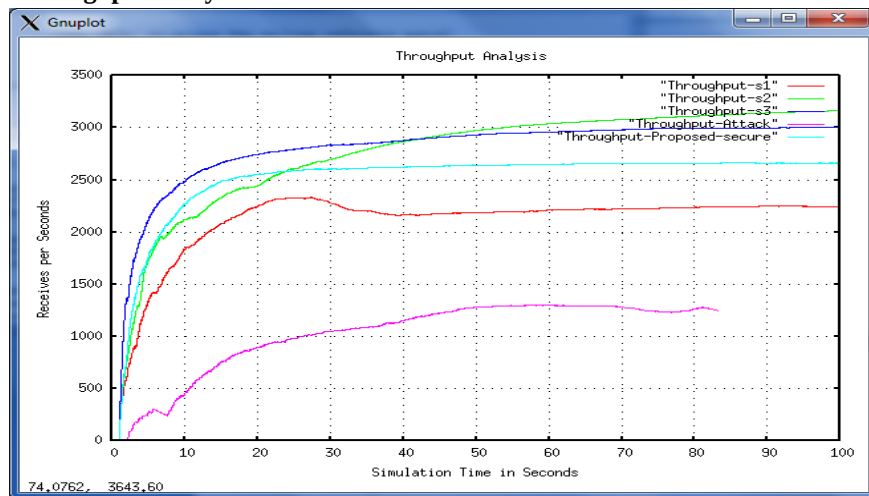


Fig. 2. Throughput Performance Analysis

The throughput performance is evaluated through number of packets is received at destination in unit time. The throughput performance of remapping attacker is about 1300 pks/second up to time 83 seconds but in security scheme the throughput is enhanced about 2200 pks/sec. The performance of rest of the normal scenario is equivalent to secure routing performance and also the S2 reaches to 3000pks/sec.

5 Conclusion and FutureWork

In MANET (Mobile Ad hoc Network) mobile nodes are continuously interchanging the information in the foam of packets or bits in network. The MANET is completely dynamic network because of random motion of mobile nodes. The sender in floods request and reply packets in network for identifying destination. The attacker in network is not interacting at the time of route establishment but it directly enhances the flooding capability by that network bandwidth is unnecessary consume. Theremappingattackerbehaviorissameasthat,floodinghugeamountofpackets

unnecessarily to set their priority higher. The proposed security scheme prevents the network from attacker. In this research three normal module S₁, S₂ and S₃, one attacker module and one security module are simulated. The three normal modules are designed on the basis of different priority. The security module observe that the attacker and block their malicious activities. In proposed scheme decentralized network is looking and work like a centralized network and it easily defend and prevent from attack behaviors during mobility environment. The results show that the presence of a Remapping Attack increases the packet loss and routing load in the network considerably. The proposed security mechanism against Remapping Attack protects the network through identified the nodes priority based communication and heavy flooding of malicious node/s.

The nodes of MANET depend on one factor also i.e. node battery power or node energy. The nodes working capability is decided through remaining battery power of node/s. The energy efficient routing will surely improves the network life time in network. In future we will propose the energy efficient routing algorithm to improve network life time and also simulate remapping attack effect on energy consumption.

6 References

- [1] Jerzy Konorski and SzymonSzott: Discouraging Traffic Remapping Attacks in Local Ad Hoc Networks, IEEE Transactions On Wireless Communications, Vol. 13, Issue 7,pp-3752-3767, 2014
- [2] Chlamtac, I., Conti, M., and Liu, J. J.-N.: Mobile ad hoc networking: imperatives and challenges. Ad Hoc Networks, Vol 1, No.1, pp. 13–64, 2003
- [3] Nema, A., Tiwari, B., & Tiwari, V.: Improving Accuracy for Intrusion Detection through Layered Approach Using Support Vector Machine with Feature Reduction. In Proceedings of the ACM Symposium on Women in Research 2016 (pp. 26-31). ACM, 2016.
- [4] Bing Wu, Jianmin Chen, Jie Wu, MihaelaCardei: A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks, Wireless/Mobile Network Security, Springer,pp-103-135, 2006
- [5] Abhay Kumar Rai, Rajiv RanjanTewari, Saurabh Kant Upadhyay: Different Types of Attacks on Integrated MANET-Internet Communication, International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3),pp-265-274 2010
- [6] K.P.Manikandan, Dr.R.Satyaprasad, Dr.K.Rajasekhararao: A Survey on Attacks and Defense Metrics of Routing Mechanism in Mobile Ad hoc Networks, International Journal of Advanced Computer Science and Applications, Vol. 2, Issue.3,pp-7-12, 2011
- [7] HimadriNathSaha , Dr. Debika Bhattacharyya , P. K.Banerjee: Study Of Different Attacks In Manet With Its Detection & Mitigation Schemes, International Journal of Advanced Engineering Technology IJAET/Vol.III/ Issue I,pp-383-388 2012
- [8] ShikhaJain : Security Threats In Manets: A Review, International Journal on Information Theory (IJIT), Vol.3, No.2, 2014
- [9] SupriyaTayal , Vinti Gupta: A Survey of Attacks on Manet Routing Protocols, International Journal of Innovative Research in Science, Engineering and Technology,Vol. 2, Issue 6,pp-2280-2285, 2013
- [10] Sk.RahimaSulthana, D.Srujan Chandra Reddy,T.Bharath Manohar: An Efficient Mechanism of Handling MANET Routing Attacks using Risk Aware Mitigation with Distributed Node Control, International Journal of Modern Engineering Research (IJMER) Vol. 3, Issue. 5 , pp-2996-3004, 2013
- [11] Sevil Sen,, John A. Clark: Evolutionary Computation Techniques for Intrusion Detection in Mobile Ad Hoc Networks, Computer Networks 55,pp-3441-3457, 2011
- [12] Gagandeep, Aashima, Pawan Kumar: Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review” International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Vol.-1, Issue-5, 2012
- [13] Er.KiranNarang, Sonal: A Study of Different Attacks In Manet and Discussion about Solutions of Black Hole Attack On AODY Protocol, International Journal Of Advanced Research In Computer Engineering & Technology Vol. 2, Issue 4,pp-1601-1606, 2013