Making Wireless infra structure less medium intrusion free

Meenu kamboj[1] , Ashwani [2]
[1,2]IIHS Kurukshetra University Kurukshetra, INDIA

Abstract : *Wireless medium is very prone to attacks of various types. Here a wireless medium has been taken into account and it has been classified as Wireless infra structure less medium. Most of the cases, it is termed as Ad hoc as well. Objective of the paper is to identify a malicious node that can enter in a routing process and can cause major damages to packet delivery. In this paper, efforts have been made for how to add intrusion detection into wireless networks, and then presenting a technique as a n algorithm for detecting attacks related to routing on these networks. Efforts have been made to develop an algorithm to detect a malicious entry and then regenerate a path to have smooth packet delivery.*

Keywords: Wireless networks, routing, adhoc, shortest path, security

1. INTRODUCTION

The very fast advancement of ad-hoc networks has mostly offered an adaptable, minimal expense answer for checking basic foundation. For instance, ad-hoc networks helps in applications like traffic checking, building observing, and front line reconnaissance [1]. The ad-hoc network plays a basic part to play in identifying these attacks, and consequently can turn into an objective for attack by its own doing. Notwithstanding, the issue of recognizing attacks, ad-hoc networks has not been tended to in the writing. A vital fascination of ad-hoc networks is their simplicity of establishment and activity. Security is one of the critical issues to develop a strong and dependable ad-hoc network [2]. Presently, most of the work done on security in ad-hoc networks has zeroed in on anticipation methods, for example, secure routing protocols, cryptography, and authentication techniques [3,4]. Ad-hoc network conventions are confronted with extra difficulties because of intricacies like a remote access medium, capricious hub development, and inconsistent hub activity. These difficulties make extensive potential to take advantage of shortcomings in the organization. Interruption discovery is the issue of recognizing misuse of PC frameworks and organizations [5]. Most IDSs apply signature-based strategies. More significantly, identifying new kinds of attacks whose marks might vary from is troublesome those in its unmistakable set. This has persuaded examination into solo learning strategies, which don't need named information and can recognize already "concealed" attacks. Rather than learning the mark of attack traffic, unaided oddity location strategies zero in on learning the mark of typical traffic. Unaided learning procedures do not need the information to be marked, nor do they require the information to be simply of one kind, i.e., ordinary or on the other hand attack traffic. This is a critical advantage over the directed learning approach. Rest of the paper has been organised as : section 2 represents traditional intrusion detection modules as literature survey. Section 3 highlights requirements for detection, Section 4 is proposed plan and last section concludes the work.

2. CONVENTIONAL INTRUSION DETECTION MODULES

The overall interruption detection system essential module involves the accompanying modules.

1. Data assortment: This module does the occupation of gathering information like packets sent, destination sequence number and different measurements which could be general to MANETS or could be intended for a convention being utilized. Contingent upon the sort of IDS or the method utilized by the IDS information could be gathered by every individual node for its environmental elements or could be gathered by unambiguous nodes which have been appointed crafted by information assortment.

2. Data handling: This module is answerable for handling the gathered information to observe the examples which show some unusual movement, exclusively processes information to track down infringement of certain standards and infer specific measurements to either choose the event of pernicious action at individual level or give the data to a higher dependable node.

3. Intrusion detection and mitigation: This module induces from the information, what sort of attack it is and which is the guilty party node. Makes the choice about the move that will be taken so the noxious node might be punished. The recognizable proof of an attack might be finished by a singular node and it might send a caution to neighborhood or it very well may be a general node given liability regarding distinguishing interruption in the event that occurring and private every one of the nodes under its locale about which is the vindictive node and how is to be moderated the attack.

3. REQUIREMENTS FOR AN INTRUSION DETECTION SYSTEM

Any intrusion detection system should satisfy specific arrangement of prerequisites
1. Intrusion detection system play out its errand utilizing least required system assets like battery power, computational force of the node on which conveyed.
2. It ought to create just impressive measure of control messages for its execution to speak with different nodes so the generally accessible scant data transmission isn't exhausted. So transmission capacity is significantly made accessible for information correspondence.
3. It shouldn't acquaint new openings for attacks with the system.
4. Performance of IDS ought not be impacted by changing node versatility, geography of the MANET
5. If it an agreeable or progressive based arrangement then it ought to take care that the conclusive nodes obligation is pivoted uniformly among every one of the nodes so that computational over-burdening isn't finished.

4. PROPOSED ALGORITHM

This section discusses the algorithms that have been proposed and implemented for identifying intruder malicious nodes in a MANET. Implementation has been done using NS2 simulator which is one of the most prominent tool used for implementation amongst researchers. Mostly solutions that have been proposed by researchers apply techniques which work on the audit data collected from the operational network and for this purpose collaborative effort is made by all the nodes in the network. Solutions that have been proposed by researchers are computational intensive and require lot of control information to be exchanged between the nodes during network operations which consume scarce resource that is bandwidth and also computations are time expensive.

Algorithm:
Protocol on which changes have been incorporated are AODV. To make the process trustworth and more realistic it has been assumed that Source and Destination nodes are secured and not malicious.

Step1. Route Request occurs form Source to a destination node
Broadcast route request (RREQ) message as normal AODV operation.

Step2. Reply messages acknowledged .
Source node collects all the route reply (RREP) messages it gets in response to the RREQ message broadcasted in step1.

Step3. Loop for message 1 to n., Where (n is the total number of received RREP messages)
If the RREP message is from Destination node
Store this message separately.
else
Store RREP message in a table called Final-RREP-table

Step4. If RREP from Destination node is not received by source node

Follow step5 to step 9
Else
Follow step10 to step12.

Step5. Apply Destination Sequence number
Consider Destination sequence numbers in RREP messages in Final-RREP-table as input
Obtain two arrays of destination sequence numbers and hence two arrays of related node information

Step6. Insert all the RREP messages to a table called malicious-Table.
Step7. Apply
Consider Hop count of RREP messages in intermediate-RREP-table as input
Obtain two arrays of Hop count and hence two arrays of related node information

Step8. Update Route table
Appends all the RREP messages from the array to malicious-table
Step9. Send data
send data to destination through intermediate node except those in malicious-table.
Step10. Apply
Take Destination sequence numbers in the RREP messages in Final-RREP-table as input
Keeping Destination sequence number of RREP message received from destination node
.
Obtain two arrays of destination sequence number and hence two arrays of related node information

Step11. Update Route
Inserts all the RREP messages from the array to a table called malicious- table

Step12. ***Choose to send data to destination through node except those in malicious-table.***

SIMULATION RESULTS

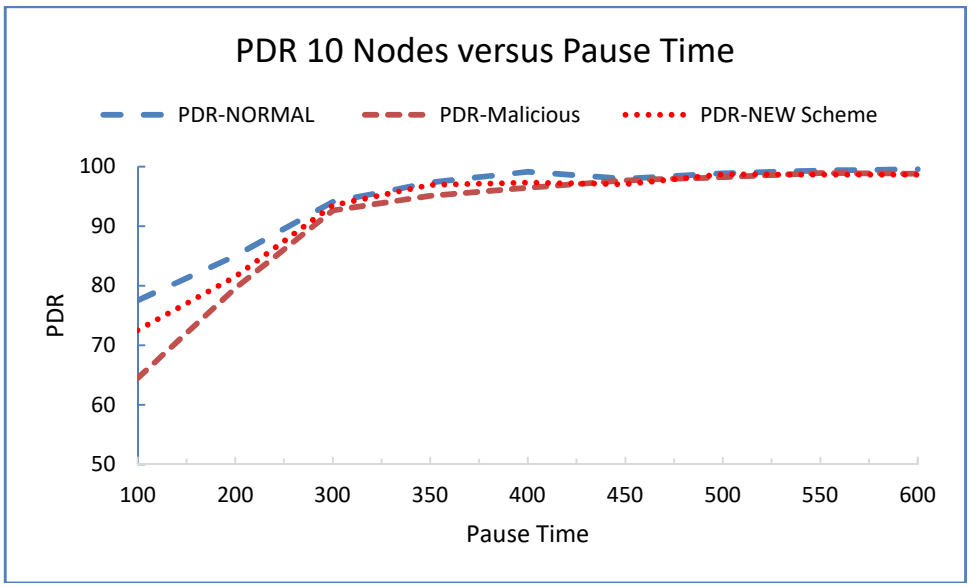
The ad hoc environment is accessible to both legitimate network users and malicious attackers. Moreover, as the wireless links are highly error prone and can go down frequently due to mobility of nodes, therefore, stable and secure routing over MANET is still a very critical task due to highly dynamic environment. An effort has been carried out to propose a NEW Scheme by taking AODV as base protocol. Experimental analysis of NEW Scheme and AODV has been done by carrying out simulation over Network Simulator (*Version:* NS-2.34). The results have been derived by using self-created network scenarios for varying number of mobile nodes. The scenarios have been generated using tcl script and the output is analyzed using trace and nam files. The same scenarios are executed for both the protocols to evaluate their performance. The performance metrics used for analysis are packet delivery ratio, average end-to-end delay, network throughput. Based on the experimental analysis, recommendations have been made about the significance of either protocol in various situations. It has been concluded that the proposed protocol i.e. NEW Scheme provides a robust, stable and secured routing strategy for adhoc cases. Varying number of UDP connections/traffic agents have been used to analyze the traffic. The mobility model used is random waypoint model in a square area. The area configurations used are 670 meter x 670 meter for 10 nodes. The packet size is 512 bytes. The simulation run time is 600 seconds

Scene-1 : 10 nodes Packet Delivery ratio w.r.t. Pause time

Area considered is 670 × 670 and simulation run time is 600 seconds during pattern analysis of 10 nodes using TCP traffic agents both with respect to varying speed and pause time. Random waypoint

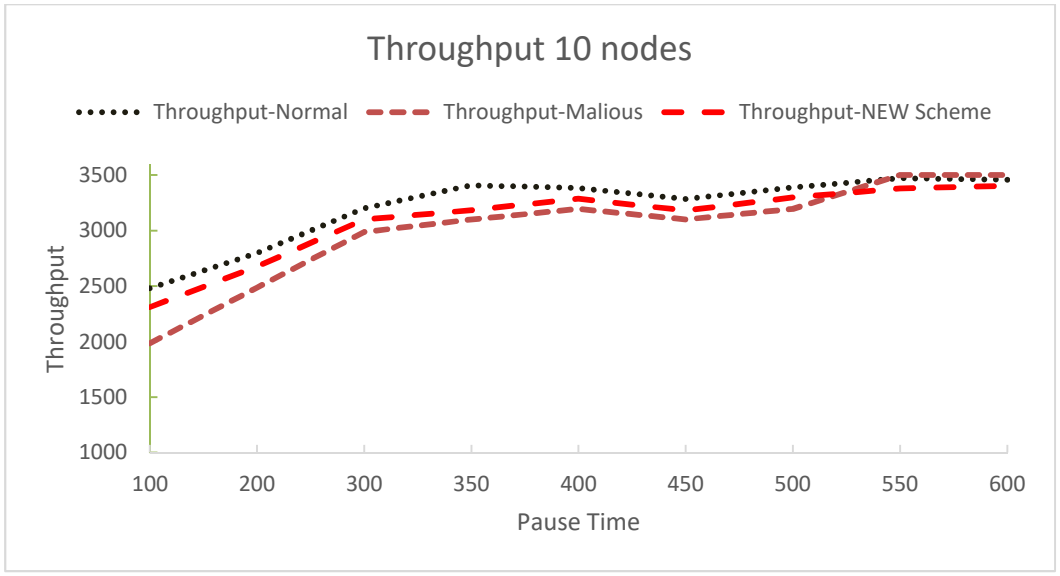
model is used. Connections using agents to transfer data are 3. Speed has been maintained at 1 meter per second. Pause time has been varied from 100 to 600. Where pause time of 100 shows maximum movement and 600 shows almost very late movement of nodes. Three parameters or metrics used are Packet delivery ratio, End to end delay and Throughput.

Graph-1 is representation of Packet delivery ratio calculated with pause time varying. Pause time of 100 means faster movement i.e. nodes start moving exactly after 100 ms and 600 shows least movement as nodes start moving at 600 ms. It is clear from Graph that In Normal case, PDR is high and reaches almost 100 percent. When a Malicious Node enters, data packet loss occurs and there is fall in PDR. Proposed scheme then takes care of the delivery ration and graph shows it. At high pause time where movement of nodes is slow then proposed scheme touches the Mark of normal case as well.

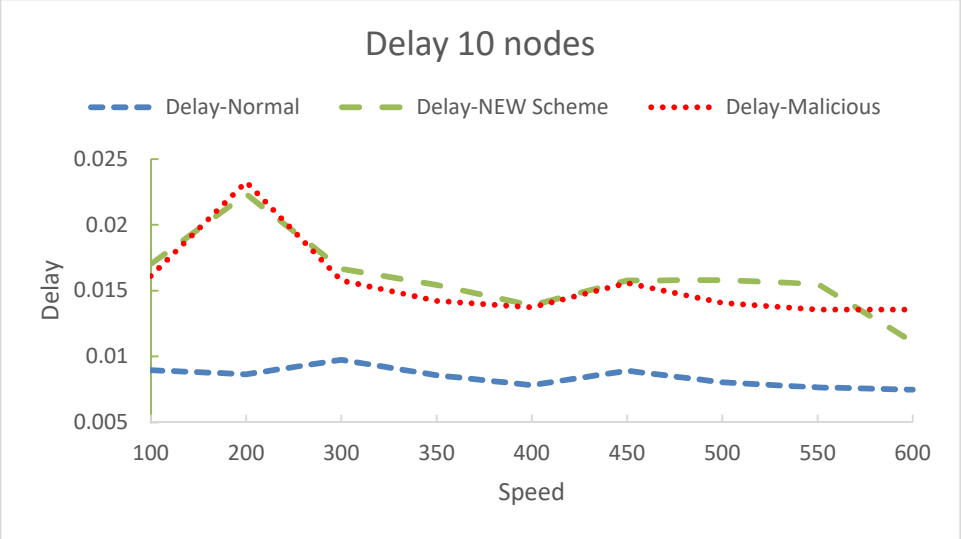


Graph1 : PDR with Pause time and 10 nodes

Graph 2 is representation of Throughput calculated with pause time varying. Graph 3 is representation of average end to end delay caused in transfer of packets from source to destination.



Graph 2 : Throughput with pause time and 10 nodes



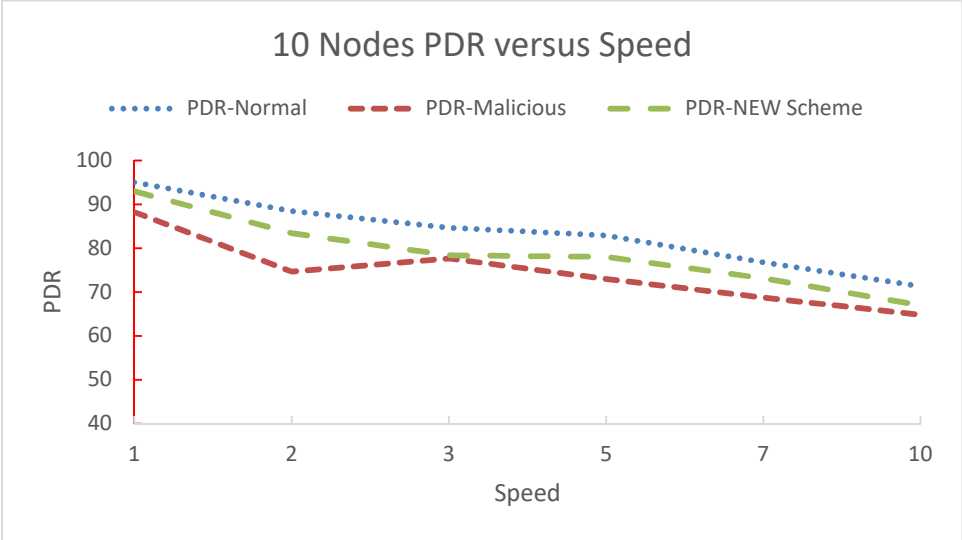
Graph 3: Delay with pause time and 10 nodes

The graph is representation of end to end delay with respect to pause time. It is very clear that in Normal case i.e. in normal AODV, though the delay occurs, but it is nominal as protocol is able to find new route quickly. In case of malicious nodes, there is more delay, it is caused actually by non reply of destination nodes, or more so by no reply messages by broken route. This has been tried to resolve using New scheme. As shown in graph there is more delay than Normal case, but is very genuine as New scheme make more calculations in finding out optimum route and then updating route tables. So delay is more but definitely it is justified as it gives more packets at delivery.

Scene-2 : 10 nodes Packet Delivery ratio w.r.t. Speed

Area considered is 670 × 670 and simulation run time is 500 seconds during pattern analysis of 10 nodes using TCP traffic agents both with respect to varying speed and pause time. Speed has been taken as variant from 1 meter per second to 10 meters per seconds. Pause time has been fixed at 100. Where pause time of 100 shows maximum movement of nodes.

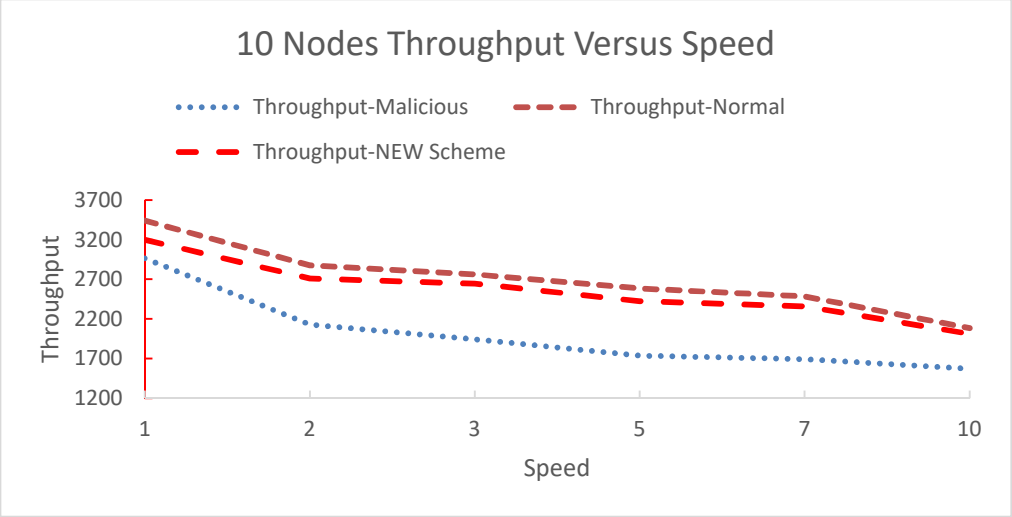
Graph 4 is representation of Packet delivery ratio calculated with speed varying. Speed of a meter per second shows slower movement where as speed of 10 meters per second means faster movement i.e. nodes start moving as a car moving in a street at a speed of appx 20 miles per hour.



Graph 4: PDR with speed and 10 nodes

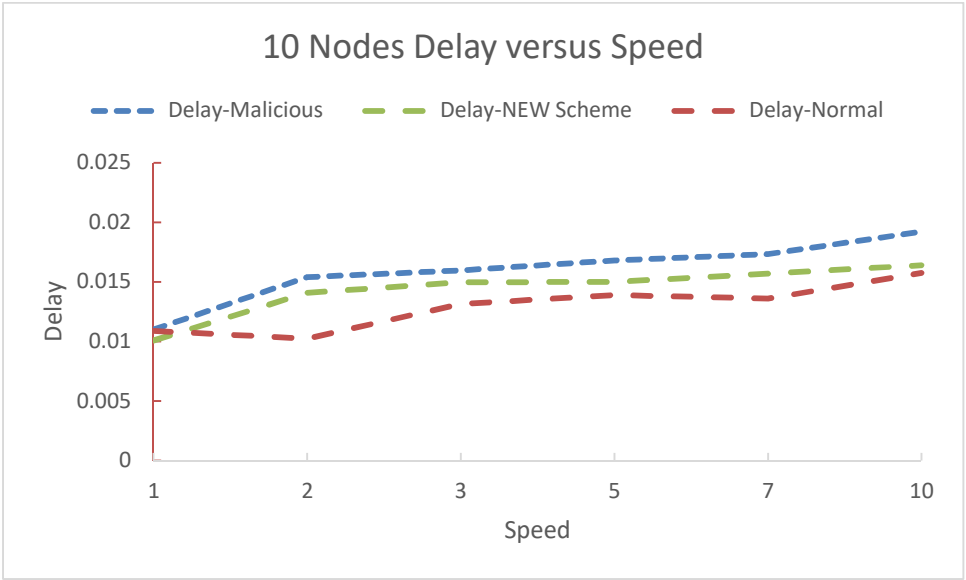
It is clear from Graph that In Normal case, PDR is high and reaches almost 100 percent. When a Malicious Node enters, data packet loss occurs and there is fall in PDR. Proposed scheme then takes care of the delivery ratio and graph shows it. At high speed time where movement of nodes is very fast then proposed scheme touches the Mark of normal case as well. It is clear that as speed increases there is more drop in PDR , this is case because faster movements causes more route breaks and more drops.

Throughput can be termed as packets delivered per unit time. Graph -5 is representation of Throughput calculated with speed varying.



Graph 5 : Throughput with speed and 10 nodes

The graph shows throughput with speed as a function. New scheme is able to touch the Normal AODV scheme almost touching same level by 2m/s onwards. It is obvious that malicious node causes drop but new scheme is able to resolve issue very quickly and reaches to maximum potential very soon.



Graph 6: End to end delay with speed and 10 nodes

End to end delay is average delay caused in reaching of packets from Source to destination each time. It is very clear that in Normal case i.e. in normal AODV, though the delay occurs, but it is nominal as protocol is able to find new route quickly. In case of malicious nodes, there is more delay, it is caused actually by non-reply of destination nodes, or more so by no reply messages by broken route. This has been tried to resolve using New scheme. As shown in graph there is more delay than Normal case, but is very genuine as New scheme make more calculations in finding out optimum route and then updating route tables. So delay is more but definitely it is justified as it gives more packets at delivery.

Conclusion

The objective of developing NEW scheme was to build up a secure and stable routing strategy for MANET. The optimum and robust route selection over ad hoc networking environment has been done using this protocol by taking into consideration the security and stability attributes. After all the performance metrics evaluation for NEW Scheme and AODV, it has been found that the performance of NEW scheme is much better than that of Malicious or intrusion effected AODV. Therefore, the ultimate goal to develop a secure and stable routing strategy for MANET has been successfully achieved.

References

1. C.Y. Chong and S. Kumar, "Sensor networks: evolution, opportunities, and challenges," in Proceedings of the IEEE, Vol. 39, No. 8, August 2003, pp. 1247–1256.

2. A. Perrig, J. Stankovic and D. Wagner, "Security in wireless sensor networks," in Communications of the ACM, Vol. 47, No. 6, June 2004, pp. 53–57.

3. J. Undercoffer, S. Avancha, A. Joshi, and J. Pinkston, "Security for sensor networks," in Proceedings of the 2002 CADIP Research Symposium, October 2002.

4. V. Yegneswaran, P. Barford and J. Ullrich. "Internet intrusions: global characteristics and prevalence," in Proceedings of ACM SIGMETRICS, June 2003, pp 138–147.

5. S. Smaha1, T. Grance, D. Teal, and D. Mansur, "DIDS (Distributed Intrusion Detection System). Motivation, Architecture, and an Early Prototype," in Internet besieged: countering cyberspace scofflaws, ACM Press, 1998.

6. Arun, A.kush, "TCP and UDP based performance evaluation of AODV and DSR routing protocol on varying speed and Pause time in MANET", International Journal Advances in Intelligent systems and Computing , Springer Publication, Next Generation Networks, Vol 6- 38, Singapore, Pp 323-332, ISSN 2194-5357. ",

7. Arun, A. Kush, "Assessment of Routing Protocols in MANET, International Journal of Computer science and Communication , Vol 7 issue 2, Pp 252-257, ***IJCSC*** *ISSN, 0973-7391, March 2018*

8. Deepak, A.Kush, "Intrusion Detection using RREP Messages of AODV Routing Protocol" ,International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 9 pp. 1956-1961 . 2017 ***Scopus Indexed***