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 fuse intrusion detection into wireless networks and present a technique for detecting novel routing attacks 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 advancement of ad-hoc networks offers the guarantee of an adaptable, minimal expense answer for checking basic foundation. For instance, ad-hoc networks have been proposed for applications like traffic checking, building observing, and front-line reconnaissance [1]. In any application including basic foundation, there is the potential risk of malicious attacks on this infrastructure, either for monetary benefit or as a psychological militant demonstration. 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. Notwithstanding, security is one of the critical difficulties to making a strong and dependable ad-hoc network [2]. Presently, most examination on security in ad-hoc networks has zeroed in on anticipation methods, for example, secure routing protocols,

cryptography, and authentication techniques [3]. These security systems are generally the primary line of guard. Be that as it may, experience with the Internet has shown that flaws in these protocols are continuously being found and exploited by attackers [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. As a general rule, signature-based methods test for highlights of realized network attacks. This brings up the issue of how to learn these highlights for known attacks, and how to recognize new attacks. It is challenging to utilize directed learning in this unique circumstance, since marked preparing information is costly to create. 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.INTRUSION DETECTION MODULES

Intrusion detection systems relying on the technique utilized can be comprehensively ordered to be independent interruption systems, cooperative intrusion detection systems and hierarchical intrusion detection systems. These characterizations depend on whether the choice is taken on individual premise or agreeably in a joint effort with neighbors choice is taken by significant level nodes. Analysts have proposed calculations that apply information mining strategies, brain organizations, master systems, signature based, AI, trust based and so forth. The proposed calculations could be investigating the review trail information, or it very well may be taking choice on the fly however every system has its advantages and disadvantages and taking special care of all sort of attacks is undeniably challenging.

There are not many proposed strategies which have proposed changes to existing organization layer convention principles to consolidate interruption detection abilities. These are ordinarily irregularity-based methods which recognize deviation from ordinary working of convention to distinguish vindictive action. Network layer conventions for MANETs have errand of tracking down a course for communication among source and objective because of portability this is certifiably not a one-time work and is done at whatever point requested by a source node not knowing way to objective. Conventions assume that the nodes in the organization are dependable, solid and agreeable and thusly have no security-based measure consolidated in their handling.

3.REQUIREMENTS FOR AN INTRUSION DETECTION SYSTEM

Remembering the issue of restricted assets accessible in MANETs and the limited available bandwidth, arrangements proposed in this theory implant into the routing protocol and don't force computational upward and communication upward, which are the best necessity for an intrusion detection system. According to writing previously proposed methods to a great extent really do review information investigation which is done at the singular level or should be possible by designated nodes and later the discoveries are given to other people. This isn't intelligent with the essentials of a versatile mobile ad-hoc network which is characterized as consortium of independent cell phones. Independence of a device is negated when definitive power is removed and it turns out to be all the more near a client server sort of climate. Strategies that have been proposed for intrusion detection work at individual level and they work just at the time when route discovery is in progress. The proposed arrangements are inconsistency based and needn't bother with any system preparing and accordingly require no verifiable information.

One of the most famous and laid out convention named AODV (Ad hoc On-Demand Distance Vector) directing convention has been viewed as which is an on-request routing protocol and a course is kept up with just when it is utilized, lapsed courses are not utilized. It is most generally utilized convention at network layer in MANETS. Proposed interruption location strategies exploit unused pieces of convention message organization to assemble data from answer messages and identify vindictive action from an ill-conceived node.

4.PROPOSED PLAN

The proposed scheme works in three phases.

In phase-1 it uses the same route selection criterion as AODV. It means a RREQ function is initiated when a Source needs to send packets to destination. RREQ follows same pattern of shortest path and reply phase. The change that has been made is that in Reply phase all nodes Sequence number which is actually the IP has been stored in Route table. Source node keeps record of which destination sequence number is provided by which intermediate node because the aim is to identify the node address i.e., nodes identity.

In Phase -2, based on Reply messages the path is created. Now if there is sudden burst of drops of packets or there is fast movement of nodes and new nodes insertion then Route tables are synchronized after each HELLO packet and route table is checked. If there are noticeable changes in sequence numbers, then Malicious intruder is detected. Because a malicious node would keep the destination sequence number sent in route reply message to be high and hop count to be low such nodes would be odd ones.

In Phase 3, the malicious node is isolated, it is marked and a new path is created. All this requires the calculations and there can be slight extra delay in packet delivery.

The normal intermediate nodes will report value of destination sequence numbers which will be same or near the destination sequence number of destination as they have active route to destination and have been forwarding or receiving data packets from the destination such nodes destination sequence numbers and hence their identity would be in an array which will be destination sequence number of the destination. Whereas malicious node report fictitious destination sequence number of destination.

Whereas malicious node report fictitious destination sequence number of destination. Source node in this case do not consider using hop count, as destination sequence number obtained from destinations route reply message is enough to identify malicious nodes. Therefore, in this case source node records the identity of intermediate nodes having destination sequence number and ensures that data forwarding will not be done through these malicious nodes.

The proposed algorithm actually creates two Arrays as MDSN called malicious destination sequence number and GDSN called genuine destination sequence numbers**.**

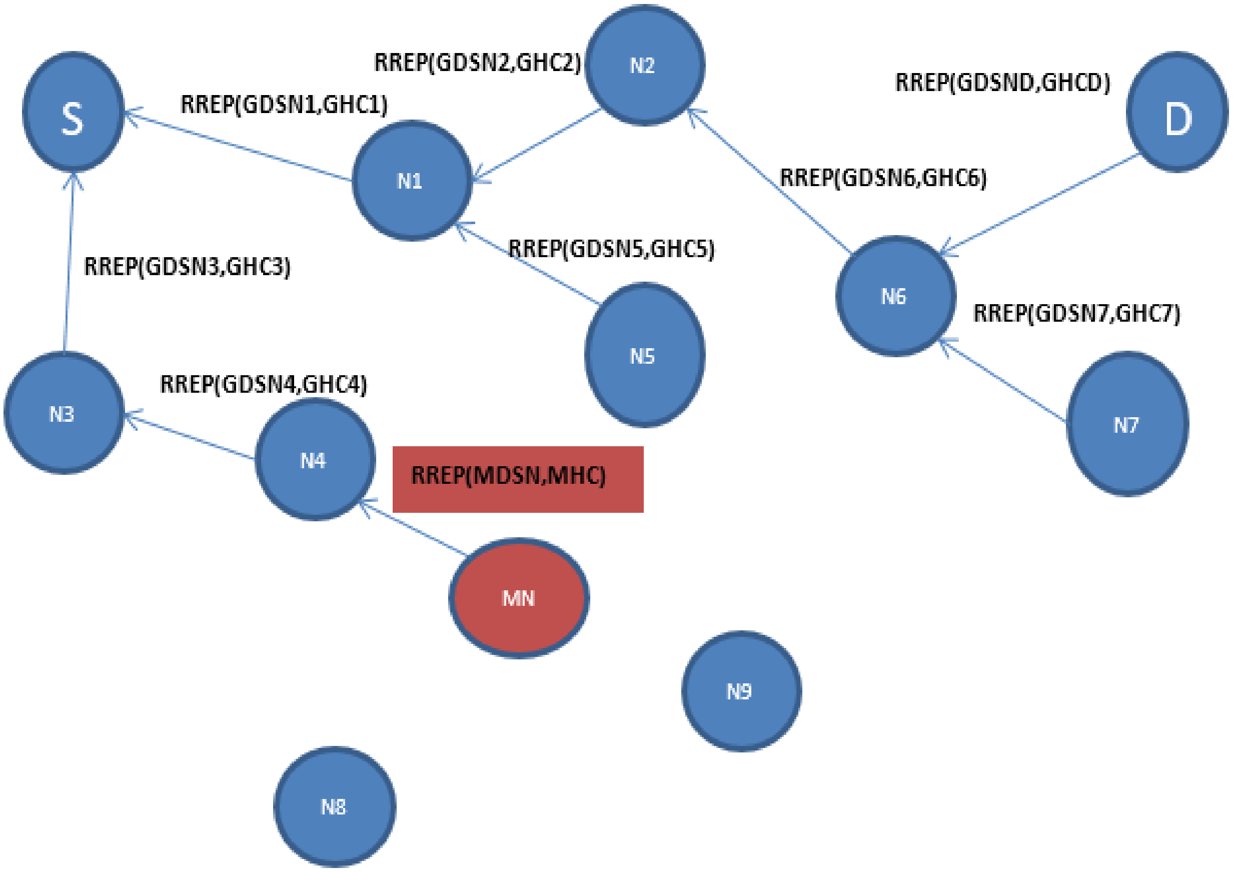
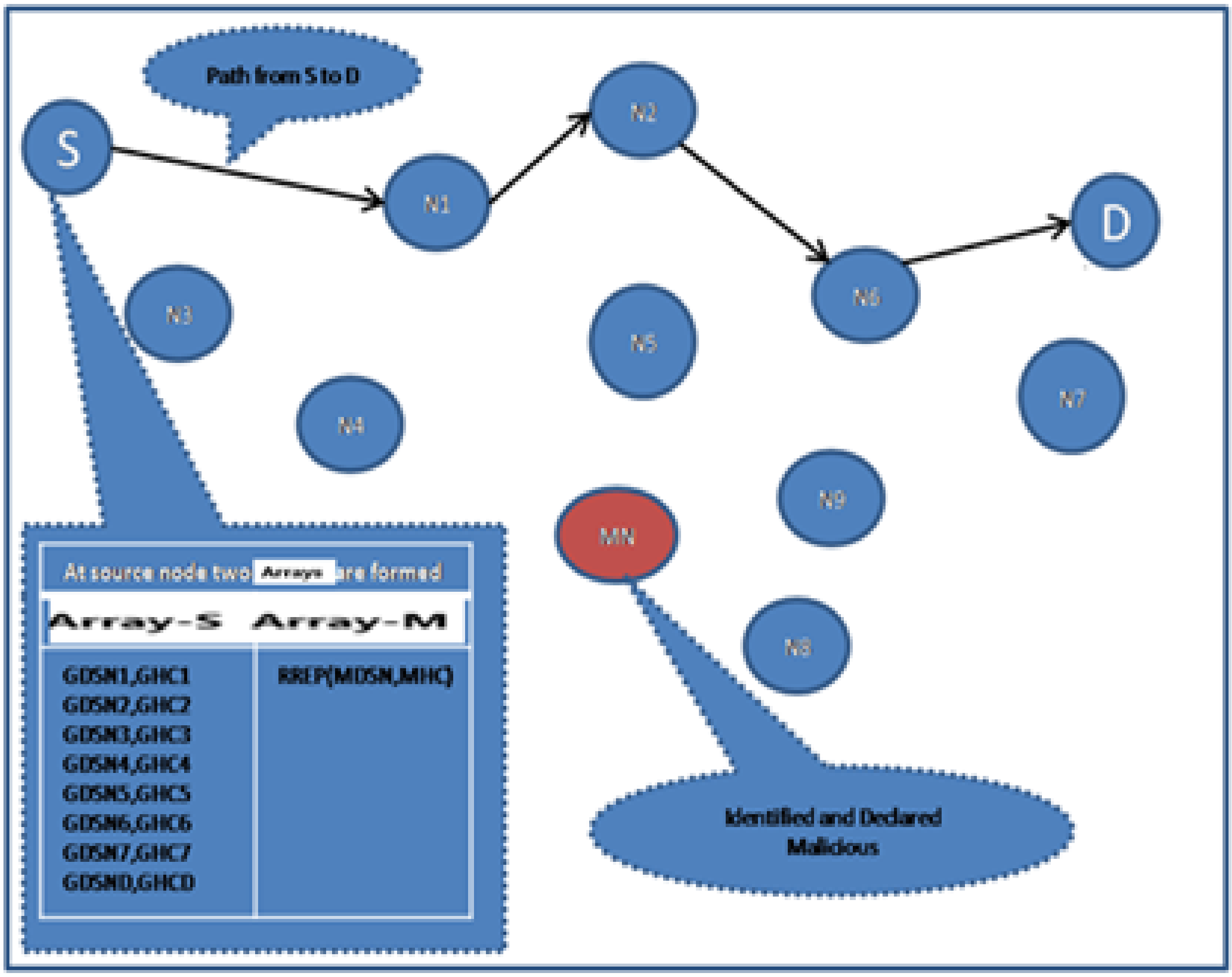


Figure shows that malicious node sends a route reply to source with false values of destination sequence number and hop count in the route reply message. GDSN implies genuine destination sequence number and GHC implies genuine hop count, whereas MDSN implies malicious destination sequence number and MHC implies malicious hop count.

Type	2 (For RREP Packet)
Flag	A - Acknowledgment required
Hop count	The number of hops from the Originator IP address to the Destination IP
Destination IP Address	The IP address of the destination for which a route is supplied
Originator IP Address	The IP address of the node which originated the Route Request for which the route is supplied.
GDSN, GHC	Genuine destination sequence number, Genuine hop count
MDSN, MHC	Malicious destination sequence number, Malicious hop count

Table: The format of the Route reply message (RREP)



SIMULATION RESULTS

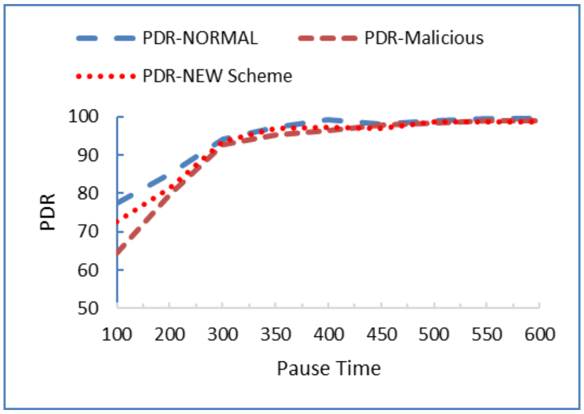
An effort has been carried out to propose a NEW Scheme by taking AODV as base protocol. Experimental analysis of NEW Scheme and AODV has been done by carrying out simulation over Network Simulator (*Version:* NS-2.34). The results have been derived by using real-life like self-created network scenarios. These are designed 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 performance metrics used for analysis are packet delivery ratio, average end-to-end delay, network throughput. It has been concluded that the proposed protocol i.e. NEW Scheme provides a robust, stable and secured routing strategy for adhoc cases.

Scene-1: 10 nodes PDR, Throughput and Delay w.r.t. Pause time and speed

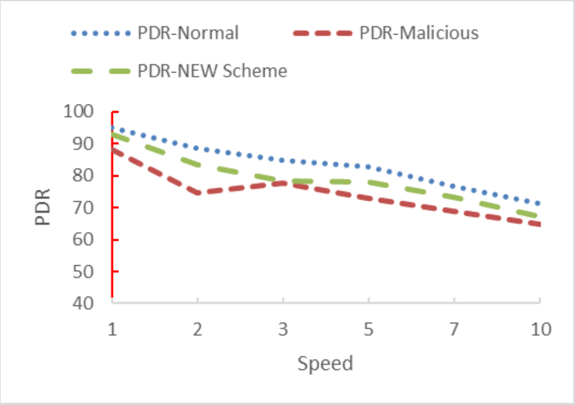
Area considered is 670 m × 670 m and simulation execution run time is 600 seconds during pattern analysis of 10 nodes using TCP and UDP traffic agents. It has been done both with respect to varying speed and pause time. Connections using agents to transfer data are 3. Speed has been maintained at 1 meter 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-1,2 is representation of Packet delivery ratio calculated with pause time and speed respectively. 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. Similarly speed os 1 m/s is slow speed and 10 m/s is faster movement. 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. Same is case with speed also, 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.

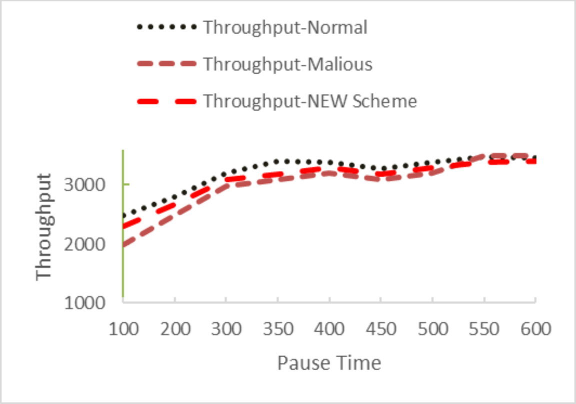


Graph 1: PDR 10 nodes with pause time as function

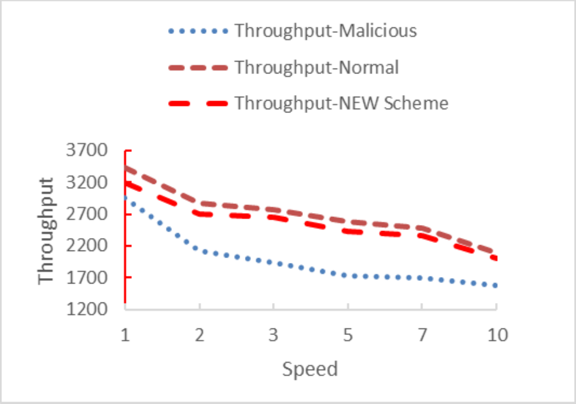


Graph 2 : PDR 10 nodes with speed as function

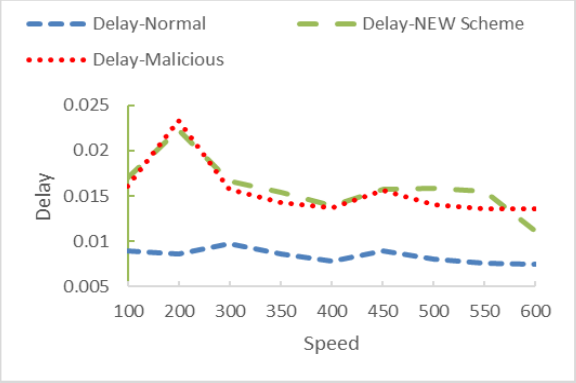
Graph 3,4 is representation of Throughput calculated with pause time and speed as functions. The graph -3 is throughput with pause time as function. Results are in line with literature. NEW scheme takes care of malicious node and recreates path and tries to achieve target. The graph-4 shows throughput 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.



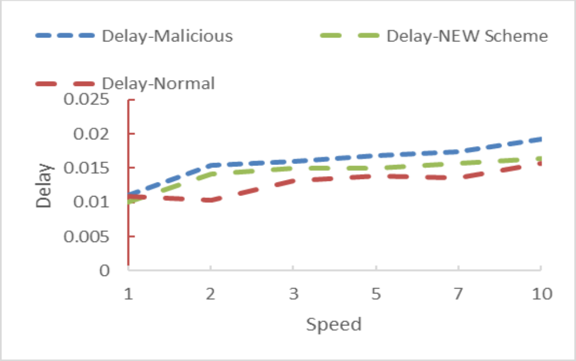
Graph 3: Throughput 10 nodes with pause time



Graph 4: Throughput 10 nodes with Speed



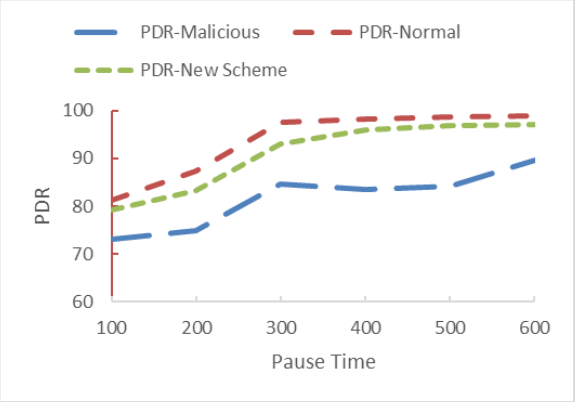
Graph 5: Delay 10 nodes with pause time



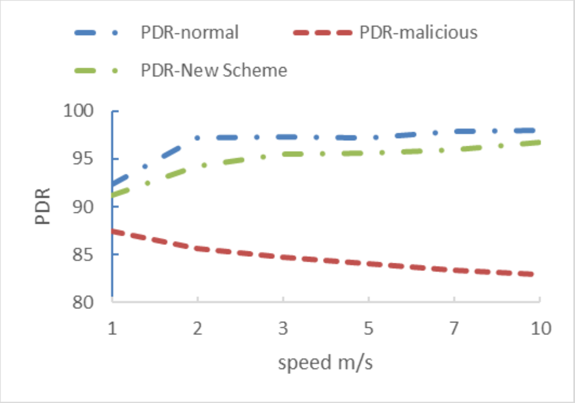
Graph 6: Delay 10 nodes with speed as function

End to end delay is average delay caused in reaching of packets from Source to destination each time. The graph 4 and 5 are representation of end to end delay with respect to pause time and speed as function. 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 : 20 nodes PDR, Throughput and Delay w.r.t. Pause time and speed

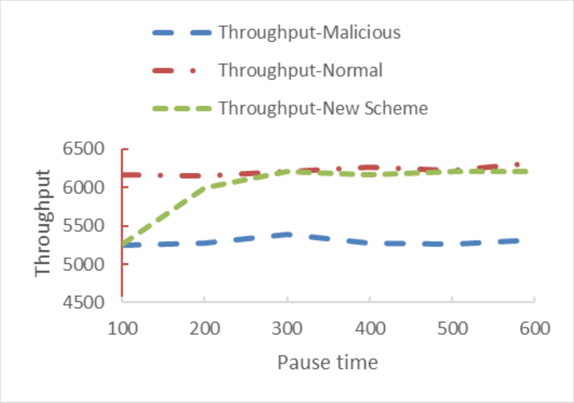


Graph 7: PDR 20 nodes with pause time

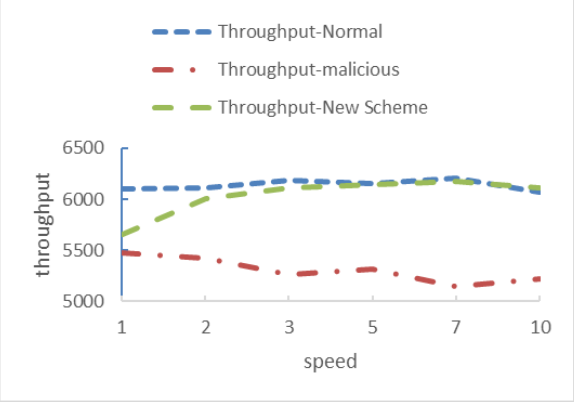


Graph 8: PDR 20 nodes with speed

Packet delivery scenario is as per literature lines in case of 20 nodes. When pause time is less there are deviations of 3 to 9 percent, but at larger pause time the NEW scheme almost touches the normal mark. Same case goes with Speed also. When speed is high there are more drops. Main concern that can be shown is that the NEW scheme is performing as per guidelines.

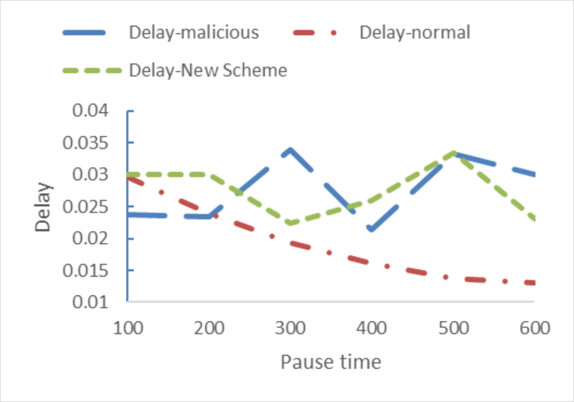


Graph 9: Throughput 20 nodes with pause time

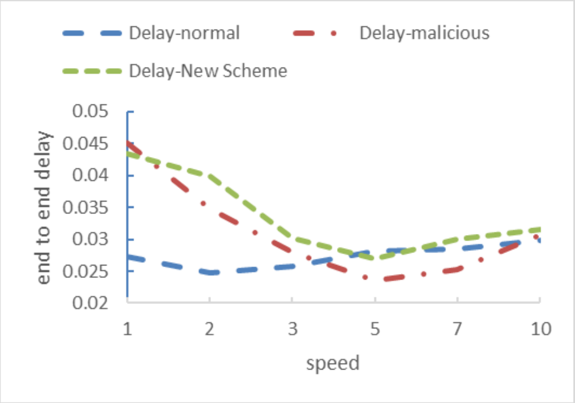


Graph 10: Throughput 20 nodes with pause time

Graph 9 and 10 are for throughput, it is clear that throughput follows almost same trend as PDR. Throughput is delivery per unit time. It almost touches the normal mark after settling down



Graph 11: Delay 20 nodes with pause time



Graph12: Delay 20 nodes with pause time

Graph 11 and 12 exhibits the end-to-end delay. It is as per the NEW scheme theory that at many instances the delay is more for NEW scheme, but it is because of new Route calculations, detecting the malicious intrusion and then removing that as well. The delay can easily be acceptable as ultimately it gives more packet delivery.

CONCLUSION

The NEW scheme based on the proposed Algorithm has been developed to have a secure and stable routing strategy for wireless networks/ the efforts have been made for MANET in particular. The best possible solution and a safe and more stable route selection has been done using this NEW Scheme. Three major metrics have been used to evaluate the NEW scheme; The comparisons have been done with existing popular scheme AODV. After all the performance metrics evaluation for NEW Scheme and AODV it has been found that the performance of NEW scheme overtakes AODV performance and performs better of Malicious or intrusion effected AODV. Therefore, the ultimate goal to develop a secure and stable routing strategy for MANET has been successfully achieved.

REFERENCE

[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. Snapp, J. Brentano, G. Dias, T. Goan, L. Heberlein, C. Ho, K. Levitt, B. Mukherjee

[6] 6.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.

[7] 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. "

[8] Arub, 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

[9] 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

[10] M. Shrivastava, "IAODV: An Improved AODV Routing Protocol for Manet," International Journal of Advanced Research in Computer Science., vol. 9, No. 2, pp. 167–174, https://doi.org/10.26483/ijarcs.v9i2, 2018.

[11] F. M. Isa, S. Saad, A. Firdaus, A. Fadzil, and R. M. Saidi, "Comprehensive Performance Assessment on Open-Source Intrusion Detection System", Springer, Singapore, 2019.