ESP IJAST
ESP International Journal of Advancements in Science & Technology
ISSN: 2583-9233 / Volume 1 Issue 1 May 2023 / Page No: 15–21
Paper Id: IJAST-V1I1P103 / Doi: 10.56472/25839233/IJAST-V1I1P103

Original Article

Increasing the Intrusion Resistance of Wireless Infrastructure

Vlaho Orperic[1], Mihovil Spanta[2]

[1,2]*University of Dubrovnik, Crotia.*

Received Date: 19 April 2023 Revised Date: 26 April 2023 Accepted Date: 03 May 2023

Abstract: *Attacks of all kinds are quite likely to occur on wireless media. In this case, a wireless medium has been considered and is being categorised as a wireless infrastructure less media. In the majority of circumstances, it is also referred to as ad hoc. The purpose of the study is to locate a hostile node that may infiltrate a routing process and seriously impair packet delivery. This research attempts to integrate intrusion detection with wireless networks and presents a method for identifying new routing attacks on them. The development of an algorithm to recognise fraudulent entries and then renew a route to ensure efficient packet delivery has been pursued.*

Keywords: *Wireless Networks, Routing, Adhoc, Shortest Path, Security.*

I. INTRODUCTION

Ad-hoc network development provides the assurance of a flexible, low-cost solution for verifying fundamental basis. Ad-hoc networks, for instance, have been suggested for uses including traffic monitoring, building observation, and front line reconnaissance [1]. Any application that uses the fundamental base is susceptible to malevolent assaults on this infrastructure, either for financial gain or as a psychological act of defiance. The ad-hoc network has a fundamental role to play in recognising these assaults, and as a result, it may become the target of an attack of its own will. Despite this, the literature has not addressed ad-hoc networks or the problem of identifying attackers. The ease of setting up and using ad-hoc networks is one of its main allures. However, one of the major challenges to building a robust and stable ad-hoc network is security [2]. The majority of research currently being done on ad-hoc network security has focused on anticipatory measures such safe routing protocols, encryption, and authentication approaches [3]. These security measures often serve as the first line of defence. But as the Internet has shown, vulnerabilities in these protocols are constantly being discovered and used by attackers [4]. Ad-hoc network conventions face additional challenges as a result of complexities such a distant access medium, erratic hub formation, and erratic hub activity. These challenges provide a lot of opportunity to exploit organisational weaknesses. The problem of identifying the abuse of PC frameworks and organisations is known as interruption discovery [5]. The majority of IDSs use signature-based tactics. Signature-based techniques often test for examples of actual network assaults. The question of how to learn these highlights for known attacks and how to spot future assaults is raised by this. In this particular situation, directed learning presents a challenge since it is expensive to provide marked preparation materials. More importantly, it may be challenging to recognise new types of assaults whose telltale signs diverge from those in its well- known collection.

This has prompted research towards solo learning techniques that can identify existing "concealed" threats without the requirement for identified information. Unaided oddity localization techniques focus on learning the mark of regular traffic rather than the mark of attack traffic. The information does not have to be tagged, nor does it have to be just one kind, such as normal or attack traffic, for unaided learning techniques to work. In comparison to the directed learning strategy, this is a significant benefit. Section 2 of the study, which serves as a literature review, depicts conventional intrusion detection modules. The third part outlines the needs for detection, the fourth presents a suggested approach, and the last portion wraps up the job.

II. INTRUSION DETECTION MODULES

Depending on the approach used, intrusion detection systems may be categorically categorised as independent interruption systems, cooperative interruption systems, and hierarchical interruption systems. These categorizations change depending on whether the decision is made on an individual basis or amicably in a cooperative effort with neighbours by substantial level nodes. Information mining techniques, brain organisations, master systems, signature-based calculations, artificial intelligence, trust-based calculations, and other methodologies have all been suggested by analysts. The suggested computations may look into the review trail data or they might make decisions immediately, but every approach has pros and cons, and guarding against all types of assaults is undoubtedly difficult.

There aren't many solutions that have been offered that would combine interruption detection capabilities by altering the conventions of the organisation layer. These are often irregularity-based strategies that differentiate between vengeful conduct and other deviations from the usual workings of convention. Because of portability, network layer standards for MANETs have the task of finding a path for communication between source and target. This is definitely not a one-time task and is completed whenever asked by a source node that is unsure about the route to the objective. Conventions presuppose that the organization's nodes are trustworthy, reliable, and pleasant and do not thus include security-based measures into their management.

III. REQUIREMENTS FOR A DETECTION SYSTEM FOR INTRUSIONS

The arrangements suggested in this theory implant into the routing protocol and do not force computational upward and communication upward, which is the best necessity for an intrusion detection system. However, keeping in mind the issue of restricted assets accessible in MANETs and the limited available bandwidth. According to writing, the approaches that were previously suggested really do, to a large part, review information research that is performed at the individual level or should be feasible by specified nodes, and then the findings are shared with others. With the fundamentals of a flexible mobile ad-hoc network, which is described as a coalition of independent cell phones, this is not clever. When decisive power is cut off, a gadget loses its independence and becomes even more similar to a client-server environment. The intrusion detection methods that have been suggested are effective at the individual level and only when route discovery is taking place. The suggested arrangements are inconsistency-based, need no system preparation, and as a result, don't call for any verified data.

One of the most well-known and well-designed conventions is the AODV (Ad hoc On-Demand Distance Vector) directing convention, which is considered as an on-request routing protocol. With this convention, a route is maintained only when it is used; expired courses are not used. In MANETS, the network layer is where this convention is most often used. Proposed interruption location solutions take use of underutilised components of standard message structure to compile information from response messages and pinpoint retaliatory behaviour by an erroneous node.

IV. PROPOSED PLAN

The suggested plan involves three stages:

The same route selection criteria as AODV is used in phase 1. It indicates that when a Source wants to deliver packets to a destination, an RREQ function is started. The reply phase and shortest route are both followed by RREQ. The modification is that all nodes' Sequence numbers, which are really IP addresses, are now recorded in the Route table during the Reply phase. Because the goal is to determine the node address, or the identity of the node, the source node maintains track of which intermediary node provides whichdestination sequence number.

Phase 2 involves creating the route based on the replies. Now, route tables are synced after each HELLO packet and route table is verified if there is a rapid burst of packet loss or if nodes are moving quickly and new nodes are added. The presence of a malicious intruder is discovered if there are obvious alterations in the sequence numbers. Because a malicious node would maintain a high destination sequence number and a low hop count in the route reply message, such nodes would be unusual.

The malicious node is separated, labelled, and a new route is established in Phase 3. Calculations are needed for everything, and there may be a little additional delivery delay.

As they have an active route to the destination and have been sending or receiving data packets from the destination, the typical intermediate nodes will report values of destination sequence numbers that are identical to or close to the destination sequence number of the destination. As a result, their identities will be stored in an array that contains the destination sequence number. Malicious nodes, however, report bogus destination sequence numbers.

Malicious nodes, however, report bogus destination sequence numbers. The destination sequence number provided from the destinations route reply message is sufficient to detect malicious nodes, hence the source node in this scenario does not consider employing hop count. Because of this, the source node in this scenario keeps track of the identities of intermediary nodes with a target sequence number and makes sure that data forwarding does not take place via these malevolent nodes. The proposed algorithm actually creates two Arrays as MDSN called malicious destination sequence number and GDSN called genuine destination sequence numbers.

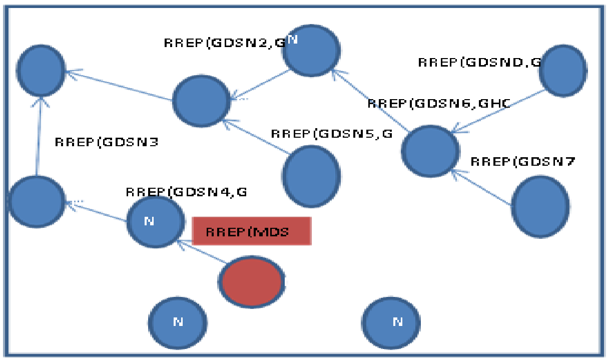


Figure 1: Block Diagram

Figure demonstrates how a malicious node sends a route reply message to the source with fictitious values for the destination sequence number and hop count. While MDSN denotes malicious destination sequence number and MHC denotesmalicious hop count, GDSN denotes genuine destination sequence number and GHC denotes genuine hop count.

Table 1: The Format of the Route Reply Message (RREP)

Type	**2 (For RREP Packet)**
Flag	A - Acknowledgmeoo6Et required
Hop count	The number of hops from theOriginator IP address to the Destination IP
DestinationIP Address	The IP address of the destinationfor which a route is supplied
Originator IPAddress	The IP address of the node which originated the Route Request forwhich the route is supplied.
GDSN, GHC	Genuine destinationsequence number, Genuine hop count
MDSN,MHC	Malicious destination sequencenumber, Malicious hop count

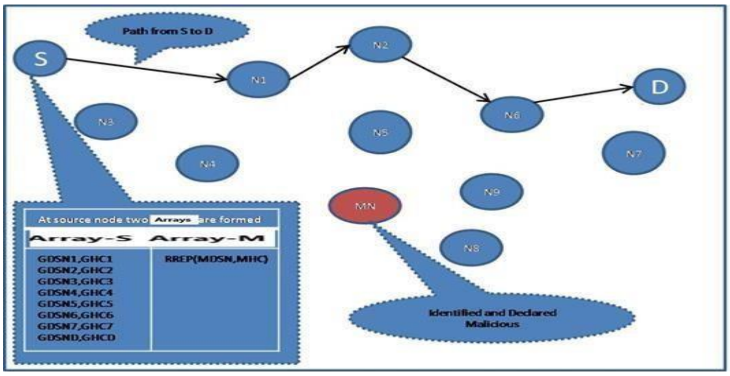


Figure 2: Array Type

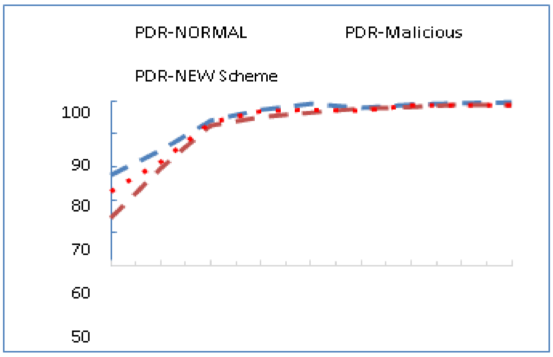
V. SIMULATION RESULTS

A proposal for a NEW Scheme using AODV as the basis protocol has been made. By simulating using the Network Simulator, the NEW Scheme and AODV have undergone experimental investigation (Version: NS-2.34). The conclusions were reached utilising network situations that were self-created and realistic. These can accommodate various numbers of mobile nodes. The scenarios were created using a tcl script, and the trace and nam files were used to examine the results. The performance parameters utilised for investigation include network throughput, average end-to-end latency, and packet delivery ratio. The suggested protocol, known as the NEW Scheme, is said to provide an ad hoc routing method that is reliable, secure, and stable.

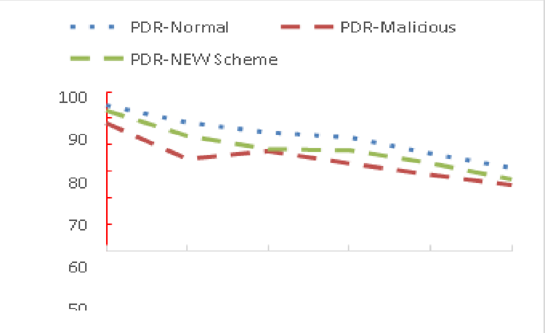
Scene 1: 10 nodes PDR, Throughput and Delay w.r.t. Pause time and speed

When 10 nodes are used for pattern analysis utilising TCP and UDP traffic agents, the area under consideration is 670 m 670 m, and the simulation execution run time is 600 seconds. Both differentiating speed and pause time have been done. There are 3 connections that use agents to transport data. One metre per second has been retained as the speed. The range of pause durations is 100 to 600. Where Maximum movement is shown by a pause time of 100, and virtually extremely late movement is shown by a pause time of 600. Packet delivery ratio, end-to-end latency, and throughput are the three variables or measurements that are employed.

Packet delivery ratio derived with speed and halt duration is shown in graphs 1 and 2, respectively. Nodes begin moving immediately after a 100 ms pause, indicating quicker movement, whereas nodes begin moving after a 600 ms pause, indicating least movement. Similary, movement at 1 m/s is sluggish while at 10 m/s is quicker. The graph makes it obvious that PDR is high and close to 100% in the normal condition. Data packet loss and a decrease in PDR happen when a malicious node joins the network. The delivery ratio is then taken care of by the proposed plan, and a graph displays it. The suggested approach also reaches the boundary of the usual situation during high pause times when node movement is sluggish. The same applies to speed; when nodes move quickly due to high speed, the suggested system similarly reaches the limits of the regular scenario. It is obvious that when speed rises, PDR decreases more; this is because quicker movements lead to more route breakdowns and declines.



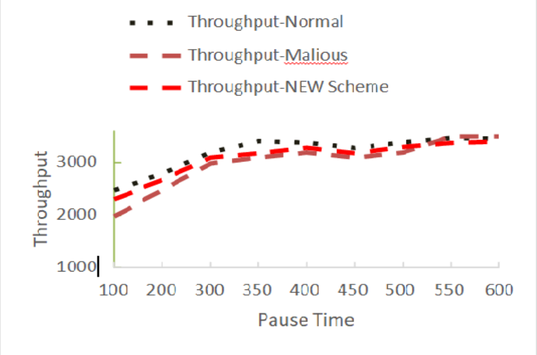
Graph 1: PDR 10 Nodes with Pause Time as Function



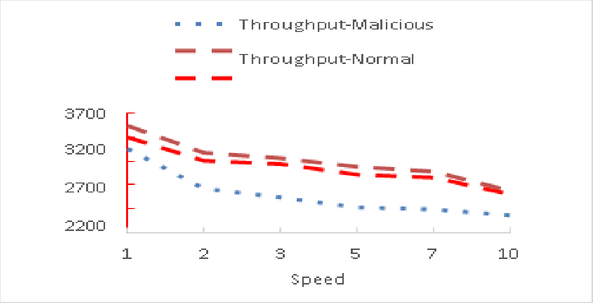
Graph 2: PDR 10 Nodes with Speed as Function

Throughput is shown in graph 3,4 using pause time and speed as functions. Throughput with pause time as a function is shown in graph -3. Results correspond to published research. The NEW method deals with the malicious node, recreates the route, and attempts to reach the destination. Throughput is shown as a function of speed in graph-4.

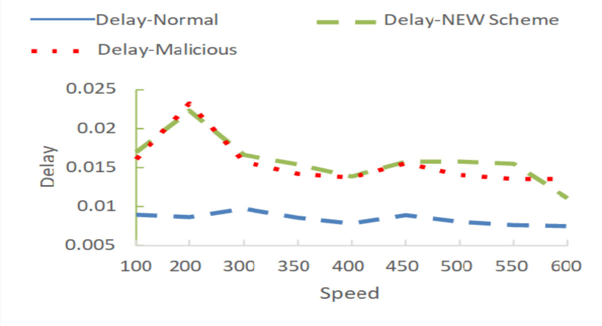
The normal AODV system can nearly be touched by the new scheme from 2 m/s forward. It is evident that rogue nodes create drops, but the new technique is able to address the problem promptly and perform to its fullest ability right away.



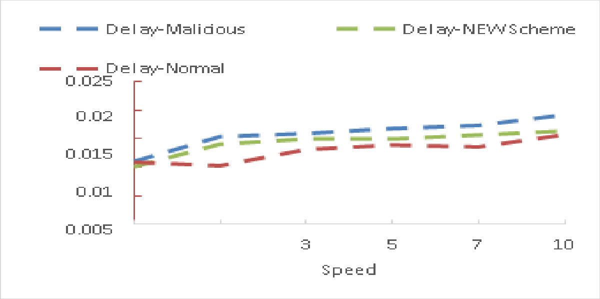
Graph 3: Throughput 10 Nodes with Pause Time



Graph 4: Throughput 10 Nodes with Speed



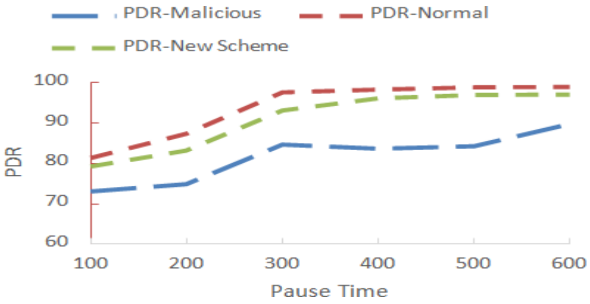
Graph 5: Delay 10 Nodes with Pause Time



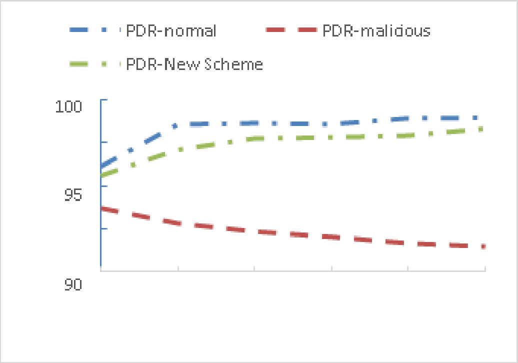
Graph 6: Delay 10 Nodes with Speed as Function

End-to-end latency is the average amount of time it takes for packets to travel from their source to their destination. The graphs 4 and 5 show the end-to-end latency in relation to the pause time and speed as functions. It is abundantly evident that in the Typical situation, or in normal AODV, a delay may occur, but it is minimal since the protocol may immediately choose a new route. In the case of malevolent nodes, there is a greater delay, which is really brought on by destination nodes that fail to respond or, more specifically, by messages that fail to be sent due to a broken route. New strategy has been used to try to fix this. As seen in the graph, there is a greater delay than in the normal situation, but this is quite real since the new approach involves additional computations to determine the best path before updating the route tables. Delay is thus greater, but it is unquestionably warranted since more packages are delivered.

Scene 2: 20 nodes PDR, Throughput and Delay w.r.t. Pause time and speed

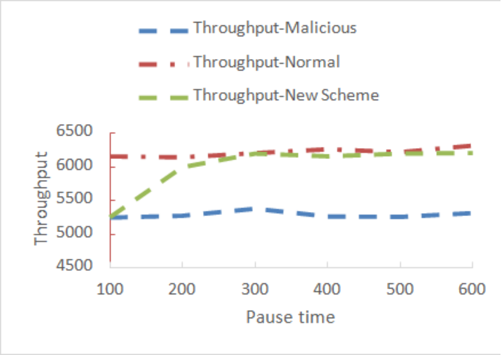


Graph 7: PDR 20 Nodes with Pause Time

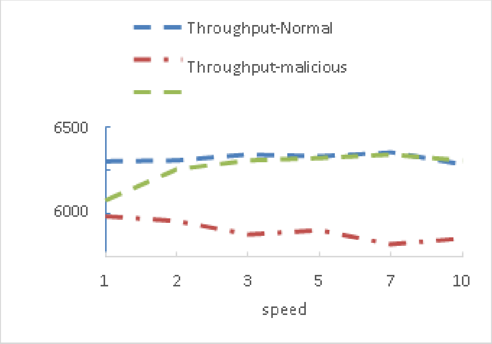


Graph 8: PDR 20 Nodes with Speed

In the case of 20 nodes, the packet delivery scenario follows the literature lines. There are variances of 3 to 9 percent when the stop period is shorter, but when the pause time is greater, the NEW scheme practically reaches the normal figure. Same case goes with Speed also. There are greater dips when the speed is high. The main issue that may be shown is that the NEW system is operating inside the parameters.

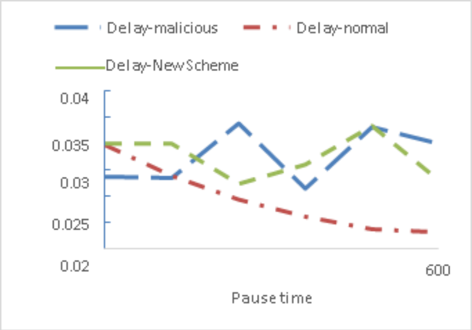


Graph 9: Throughput 20 Nodes with Pause Time

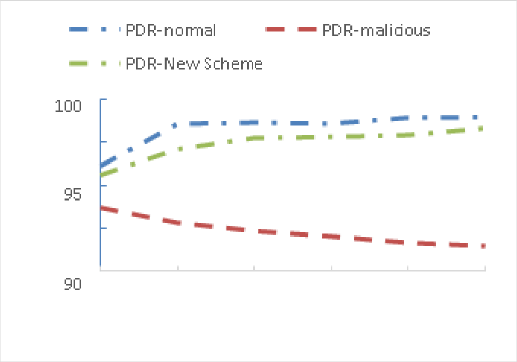


Graph 10: Throughput 20 Nodes with Pause Time

Throughput is shown in Graphs 9 and 10. It is obvious that throughput exhibits a similar pattern as PDR. Delivery per unit of time is known as throughput. It settles and nearly reaches the usual mark.



Graph 11: Delay 20 Nodes with Pause Time



Graph12: Delay 20 Nodes with Pause Time

The end-to-end latency is seen in graphs 11 and 12. According to the hypothesis behind the NEW scheme, in many cases the delay is not caused by the NEW scheme but rather by new Route computations that identify harmful intrusions and subsequently remove them. The delay is readily tolerable since it results in greater packet delivery in the end.

V. CONCLUSION

In order to have a safe and reliable routing strategy for wireless networks—and with MANET in mind—the NEW scheme, based on the suggested Algorithm, has been designed. Using this NEW Scheme, the optimal solution and a safe and more reliable route selection have been made. The NEW method has been evaluated using three key parameters, and comparisons have been made with the widely used current scheme AODV. The examination of all performance measures for NEW Scheme and AODV revealed that NEW Scheme outperformed AODV and outperformed AODV that had been maliciously or intrusively affected. Therefore, the overall objective of creating a reliable and secure routing mechanism for MANET has been accomplished.

VI. REFERENCES

[1] Buttyán, Levente, et al. "Application of wireless sensor networks in critical infrastructure protection: challenges and design options [Security and Privacy in Emerging Wireless Networks]." IEEE Wireless Communications 17.5 (2010): 44-49.

[2] Buttyán, Levente, et al. "Application of wireless sensor networks in critical infrastructure protection: challenges and design options [Security and Privacy in Emerging Wireless Networks]." IEEE Wireless Communications 17.5 (2010): 44-49.

[3] Sterne, Daniel, et al. "A general cooperative intrusion detection architecture for MANETs." Third IEEE International Workshop on Information Assurance (IWIA'05). IEEE, 2005.

[4] Nilsson, Dennis K., Ulf E. Larson, and Erland Jonsson. "Creating a secure infrastructure for wireless diagnostics and software updates in vehicles." International Conference on Computer Safety, Reliability, and Security. Springer, Berlin, Heidelberg, 2008.

[5] Kong, Jiejun, et al. "Adaptive security for multilevel ad hoc networks." Wireless Communications and Mobile Computing 2.5 (2002): 533-547.

[6] Chandrakala, Nelli, and Chelloju Raju. "Distributed Intrusion Detection Architecture Based on Clustering of the Nodes that Addresses the Security Vulnerabilities of the Ad-hoc networks."

[7] Liang, Haoran, et al. "MBID: Micro-blockchain-based geographical dynamic intrusion detection for V2X." IEEE Communications Magazine 57.10 (2019): 77-83.

[8] Zhang, Ruirui, and Xin Xiao. "Intrusion detection in wireless sensor networks with an improved NSA based on space division." Journal of Sensors 2019 (2019).

[9] Grilo, António, et al. "A wireless sensor and actuator network for improving the electrical power grid dependability." Proceedings of the 8th Euro-NF Conference on Next Generation Internet NGI 2012. IEEE, 2012.

[10] Ghosh, Sagarika, et al. "An intrusion resistant scada framework based on quantum and post-quantum scheme." Applied Sciences 11.5 (2021): 2082.

[11] Shamshirband, Shahab, et al. "Computational intelligence intrusion detection techniques in mobile cloud computing environments: Review, taxonomy, and open research issues." Journal of Information Security and Applications 55 (2020): 102582.

[12] Anantvalee, Tiranuch, and Jie Wu. "A survey on intrusion detection in mobile ad hoc networks." Wireless network security. Springer, Boston, MA, 2007. 159-180.