**A Novel Neighbor Trust Based Security Based Mechanism to Prevent Attacks in MANETs**

By Gurveen Vaseer, Garima Ghai, Pushpinder Singh Patheja and Dhruva Ghai

**ABSTRACT:** Mobile nodes in a Mobile Ad hoc Network (MANET) form a temporal link between sender and receiver due to their continuous movement in a limited area. This network can be easily attacked since there is no organized identity. In this paper we propose a Neighbor Trust Based security scheme that prevents malicious attacks viz. Probe, Denial of Service (DoS), Vampire, User-to-Root (U2R) in a MANET. The proposed security scheme identifies each node’s behavior in the network in terms of packets received and forwarded. Nodes are placed in suspicious range and if the security scheme detects malicious function continuously, then it is confirmed that the particular node is the attacker in the network. The performance of the proposed prevention algorithm has been tested in the Network Simulator-2 (NS-2) environment. To the best of authors’ knowledge, this is the first paper reporting a neighbor trust based prevention method for malicious attacks in a MANET.

1. **INTRODUCTION AND CONTRIBUTIONS**

|  |
| --- |
| C:\Users\support\Desktop\inis.png |
| **FIGURE 1.**  Importance of an attack-free environment |

The dependence of our society on the diverse applications of Information Systems is known to all. There is a constant integration of information systems with engineering fields such as aerospace, industrial systems etc. This interconnection between cyberspace and physical space poses a threat of hacking and hence damage of infrastructure [10]. Thus the need of Intrusion Detection and prevention becomes necessary for the proper functioning of the physical space. Figure 1 gives an overview of the importance of an attack-free environment for safe phones, smart grids and industrial control systems.

MANET (Mobile Ad hoc Network) is a collection of independent nodes that are mobile and able to communicate with each other wirelessly without the presence of any centralized coordinator [13]. Each node functions as a host as well as router. MANETs have numerous practical applications such as in nature disaster areas, emergency operations, battlefield communication, campus networks etc. [9]. Thus, security is a major concern in such networks, which necessitates the routing protocol to deal with attacks of certain types. In this paper, four types of attacks are analyzed i.e. Denial of Service (DoS), Probing, Vampire and User-to-Root. In a DoS attack, the system is flooded with illegitimate requests and responses making it inaccessible to legitimate users hence crashing the server [11]. In a Probe attack, a device or an activity is maliciously introduced in the system, which gains access to the system and damages it. In U2R attack, the attacker gains control of the victim machine acquiring super user privileges [12]. Vampire attack is a type of DoS attack that consumes the node’s energy and decreases the network’s efficiency and reliability [2]. A Neighbor Trust Based method is proposed to defend the attacks through two modes: suspicious and blocking to isolate the behavior of defined attack activity that breaks the security of the network.

* 1. **NOVEL CONTRIBUTIONS OF THIS PAPER:**

The novel contributions of this paper are as follows: 1) A novel intrusion prevention algorithm for a MANET is proposed. 2) For prevention, the proposed algorithm uses a Neighbor Trust Based scheme. 3) The algorithm is designed to detect Probe, Denial-of Service (DoS), Vampire and User-To-Root (U2R) attacks. 4) The results are presented using AODV protocol.

1. **DISCUSSIONS OF THE STATE OF ART**

Authors in [1] propose a scheme in which two MANETs are merged and a method called Merging Using MrDR (MUMrDR). J. Pullagura J.R. et. al. [2] generated a comparison mechanism for Vampire attacks using standard routing protocols on the network layer viz. Destination Sequenced Distance Vector (DSDV) etc. J. Vuorinen et. al. [3] discuss the importance of cyber security in today’s scenario and the complexity of security mechanisms and how top-notch security mechanisms affect the productivity cycles of data and throughput. G. Folino et. al. [4] proposed a Distributed method by condensation of very large data sets using neighbor-based techniques to encounter Probe and U2R attacks. A. Al-Roubaiey et. al. [5] propose an adaptive acknowledgment intrusion detection with node detection in MANET. [R. Shrestha](https://www.computer.org/web/search?cs_search_action=advancedsearch&searchOperation=exact&search-options=dl&searchText=Rakesh+Shrestha) et. al. [7] propose a multi-layer detection technique to detect DoS attacks by designing a cross layer architecture to control DoS attacks. Yi Gong et. al. [8] design a Multi-agent Intrusion Detection System in large switched networks to protect Industrial Control Systems.

|  |  |  |
| --- | --- | --- |
| Table I: Comparison with Related Works | | |
| **Reference** | **Work done** | **Our work** |
| [A. Alsumayt](https://www.computer.org/web/search?cs_search_action=advancedsearch&searchOperation=exact&search-options=dl&searchText=Albandari+Alsumayt) et. al [1] | Merge two MANETs based on the Monitoring, Detection, and Rehabilitation (MrDR) method to mitigate DoS attacks. | Detect and prevent DoS attacks with neighbor trust based mechanism. |
| J. Pullagura et. al [2] | Comparison of performance of standard routing network protocols for Vampire attacks. | Detect and prevent Vampire attacks using AODV protocol. |
| J. Vuorinen et. al [3] | Discuss the paradox prevailing amidst information security and its mechanisms and how too much vigilance affects absolute productivity cycles. | Detect the malicious attacks in networks using neighbor trust based algorithm design. |
| G. Folini et. al [4] | Neighbor trust based mechanism to eliminate attacks by condensation of very large data sets. | Profile based detection on the four types of attacks i.e. DoS, Probe, Vampire and U2R. |
| A Al-Roubaiey et. al [5] | Adaptive acknowledgment (AACK) for solving transmission power and receiver collision | Resolve the problem of resource utilization through trust based method. |
| R. Shreshtha et. al [7] | Multi-layer detection technique to detect DoS attacks. | Neighbor node trust approach and prevents DoS, Probe, Vampire and U2R attacks. |
| Yi Gong et. al [8] | Multi-agent Intrusion Detection System in large switched networks to protect Industrial Control Systems(ICS) | Profile based analysis method is adopted for minimization of malicious attacks. |

1. **A NOVEL SCHEME FOR SECURE MANETs**

Our proposed security mechanism checks its neighboring node for malicious activity i.e. whether the node deviates from its specific behavior. Certain checkpoints have been established to determine the nature of attack. We have used AODV protocol for network communications [14]. The main aim of protocol is routing, which is designed to build and maintain a table of route information. An AODV protocol work flow is depicted in Figure 2.

1. **Proposed Algorithm**

The proposed scheme is shown in figure 3. Data is tested using 50 nodes in a radio range of 800 X 800 m (shown in Table II). Here, I is a collection of addresses of intermediate nodes between the sender and receiver. It is compared with R (receiver nodes address) until there is a match. When the data is broadcasted from the sender (S) to receiver (R) using AODV protocol, preventer (watcher) node (W as in figure 3) is a special node that is capable of tracing the established route, observing the activity of nodes and blocking the malicious activity generator node under the specified range. The preventer node uses two primitives: suspicious and blocking. If the nodes behavior is found to be abnormal, (which does not meet the functionality of normal behavior) then it is set as suspicious node and is under full surveillance of the preventer node. If the activity of node is found to be malicious then that node is blocked by the preventer node. Preventer node plays an important role in watching all the attacks that are mentioned as follows:

Activity of U2R attack is traced by data forwarding criteria, while the intermediate node updates its self id as the receiver id. Data is not forwarded to the receiver node which drops by the LOOP (LOOP is a condition wherein the incoming and outgoing node is same; that is the node forwards itself to the next node) criteria implying that the preventer node has

|  |
| --- |
| C:\Users\Dean sir\Documents\Research\IEEE_Potentials_2018_Gurveen\aodv.png |
| FIGURE 2. AODV working flow chart |

identified the activity as U2R attack and hence blocked the attacker node. Vampire attacker node consumes extra energy of the node. When the preventer node finds that the required energy for data transmission of particular path is greater than the defined energy threshold, it further checks the energy consumption of each node in the path. When the node runs extra threads other than the data forwarding or it consumes higher energy than all other nodes combined, it is classified as a vampire attack and is blocked by the preventer node. Probe attacker node behaves correctly while the routing module executes, but in future they drop or capture the data of source node. This activity is traced by the preventer node and blocks the attacker nodes. Similarly preventer node finds out that unwanted data packet flood the network at high rate, the activities that do not match with normal are blocked. DoS attacker floods the network with a number of junk packets in order to overload the system, so that legitimate requests are not fulfilled. Thus the preventer node checks the data packet and if it does not match standard TCP, UDP headers (as in NS-2), it compares the time instance. If the time instance is more than normal data rate then it identifies the node as faulty node and hence blocks it. Given below is the Flowchart of our proposed scheme that is divided into 3 steps viz. Step 1, Step 2 and Step 3.

|  |  |
| --- | --- |
| C:\Users\Dean sir\Documents\Research\IEEE_Potentials_2018_Gurveen\step1.png | |
| C:\Users\Dean sir\Documents\Research\IEEE_Potentials_2018_Gurveen\algo2.png | C:\Users\Dean sir\Documents\Research\IEEE_Potentials_2018_Gurveen\algo3.png |
| **FIGURE 3.** Flowchart of the proposed algorithm | |

1. **RESPONSE OF NETWORKS UNDER THE PROPOSED SECURITY SCHEME**

|  |  |
| --- | --- |
| Table II: Network Simulation Parameters | |
| **Parameter** | **Value** |
| Number of nodes | 50 |
| Simulation area | 800 X 800 m |
| Routing protocol | AODV |
| Attack types | Probing, DoS, Vampire, U2R |
| Prevention | Neighbor Trust |
| Simulation time | 100 seconds |
| Transport layer | TCP, UDP |
| Traffic type | CBR, FTP |
| Packet size | 512 bytes |
| Number of traffic connections | 10 |
| Node speed | Random |

This section describes the response of the simulated network under conditions of attack as well as after applying prevention mechanism. The responses reported are Throughput, Normal Routing Load (NRL) and End-to-End Delay. The simulation parameters considered for simulation are mentioned in Table II. AODV protocol is considered for routing between sender and receiver. The simulation is performed in NS-2 simulator version 2.31, Windows 7 with Cygwin software that provides Linux environment in Windows.

*A. Normal Routing Load DoS Attack and Prevention case:*

Normal routing load (NRL) is the ratio between the number of routing packets to the total data received. Figure 4(a) shows the performance of the network under DoS attack with and without the prevention scheme. The scheme stops the unwanted congestion delay and searches for new path for the nodes so that the overhead after applying prevention is reduced and the unwanted flooding is completely removed from the network.

*B. Normal Routing Load U2R Attack and Prevention case:*

Figure 4 (b) shows the network performance with and without the prevention scheme. Here, due to dropping of packets by the attacker, the receiver does not receive data properly. Then the sender repeatedly sends the routing packets in the network to establish connection with the receiver. Due to flooding of packets repeatedly, the overhead in the network is enhanced. After applying prevention scheme performance is improved and overhead reduces as the preventer node repairs the local route in which the attacker resides and generates a new route to the destination node.

*C. Normal Routing Load Probe Attack and Prevention case:*

In Figure 4 (c), the performance of the proposed scheme against probe attack is shown. The overhead performance of Probe attack and its security scheme against probe is measured and is recognized that the attacker overhead is almost the same as the security scheme except in simulation start time and end of simulation time in network. Here the data packet loss is minimized in the prevention scheme by identifying attacker nodes and hence blocking them and channelizing a new path with the remaining nodes.

*D. Normal Routing Load Vampire Attack and Prevention case:*

The Vampire attack is flooding huge amount of packets in the network and these packets consume the most valuable resource i.e. energy of nodes in MANET. Preventer node identifies the attacker node and blocks it so that new path is found where actually no resource consumes increased energy and hence reduces NRL. Figure 4 (d) shows the overhead performance of vampire attack and proposed Vampire-Prevention scheme. The overhead after applying prevention is reduced and also the unwanted consumption is totally zero due to the effectiveness of the prevention scheme.

*E. Throughput Analysis DoS Attack and Prevention case:*

The throughput is measured in number of packets per unit time. The throughput performance is improved after applying proposed prevention scheme, as packets are tested for their behavior of UDP/TCP and if there is delayed data rate they are blocked by the proposed scheme and new path of transmitting legal packets is devised. Figure 4 (e) shows the performance of Throughput in DoS attack and prevention scenario.

*F. Throughput Analysis U2R Attack and Prevention case:*

Figure 4 (f) shows the throughput performance of the network under U2R attack with and without the security scheme. The prevention scheme checks whether the packet has not updated itself as the root node and in spite of being idle is not forwarding the data to the next hop. After ensuring these conditions, if the data packets are dropped, then that node is blocked and an alternate path is devised.

*G. Throughput Analysis Probe Attack and Prevention case:*

The performance of the proposed algorithm against probe attack is shown in Figure 4 (g). Due to dropping of packets by attacker, the receiver does not receive all the data. The attacker consumes all the data and also wastes the valuable energy resource of MANET. In the proposed prevention scheme, packets are checked if they are dropped or not forwarded. If no specific reason is provided for these actions, the nodes are blocked.

*H. Throughput Analysis Vampire Attack and Prevention case:*

In the proposed scheme, it is checked that no extra threads are used for communication in the path. Also, the time of previous node and current nodes are calculated and if it is found that the time taken by the node to move is more than that of its threshold, then it is blocked and identified as an attacker. Figure 4 (h) depicts the throughput analysis in vampire attack and prevention scenario. The attacker’s aim is to drop the packets or consume the resources of network by flooding number of unwanted packets in network.

*H. Average End to End Delay Analysis:*

Average end to end delay refers to the average time taken for packets transmission across the network from sender to receiver nodes. End to end delay depends on queue delay, bandwidth, processing and contention; if all these take higher time then end to end delay will increase. Figure 4 (i) shows the average end to end delay in different attacks scenario as well as its prevention scenario. While applying the prevention methodology the delay is minimized, because prevention methodology gives secure and efficient path. The delay in normal case is 0.33 ms. Table III shows the network performance under various attacks and their prevention schemes.

|  |  |  |
| --- | --- | --- |
| C:\Users\Dean sir\Documents\Research\IEEE_Potentials_2018_Gurveen\result\nrl_dos.png | C:\Users\Dean sir\Documents\Research\IEEE_Potentials_2018_Gurveen\result\nrl_u2r.png | C:\Users\Dean sir\Documents\Research\IEEE_Potentials_2018_Gurveen\result\nrl_probe.png |
| (a). NRL Analysis for DoS attack prevention | (b). NRL Analysis for U2R attack prevention | (c). NRL Analysis for Probe  attack prevention |
| C:\Users\Dean sir\Documents\Research\IEEE_Potentials_2018_Gurveen\result\nrl_vampire.png | C:\Users\Dean sir\Documents\Research\IEEE_Potentials_2018_Gurveen\result\throughput_dos.png | C:\Users\Dean sir\Documents\Research\IEEE_Potentials_2018_Gurveen\result\throughput_u2r.png |
| (d). NRL Analysis for Vampire attack prevention | (e). Throughput Analysis for DoS attack prevention | (f). Throughput Analysis for U2R attack prevention |
| C:\Users\Dean sir\Documents\Research\IEEE_Potentials_2018_Gurveen\result\throughput_probe.png | C:\Users\Dean sir\Documents\Research\IEEE_Potentials_2018_Gurveen\result\throughput_vampire.png | C:\Users\Dean sir\Documents\Research\IEEE_Potentials_2018_Gurveen\result\delay.png |
| (g). Throughput Analysis for probe attack prevention | (h). Throughput Analysis for vampire attack prevention | (i). End to End delay analysis |
| **FIGURE 4**: Network output responses | | |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Table III: Network Performance Summary | | | | | | | | | |
| **Simulation**  **Parameters** | **DOS** | **DOS Prevention** | **Vampire** | **Vampire Prevention** | **Probe** | **Probe Prevention** | **U-to-R** | **U-to-R Prevention** | **Normal** |
| SEND (no. of packets) | 5142 | 7450 | 3901 | 5570 | 4756 | 8330 | 1586 | 6299 | 8238 |
| RECV (no. of packets) | 4196 | 6687 | 3203 | 5067 | 3901 | 7502 | 423 | 5560 | 7458 |
| PDF (% data received) | 81.6 | 89.76 | 82.11 | 90.97 | 82.02 | 90.06 | 26.67 | 88.27 | 90.53 |
| NRL | 25.91 | 0.7 | 46.99 | 0.99 | 56.42 | 1.06 | 6.82 | 0.85 | 1.01 |
| Dropped data (no. of packets) | 946 | 763 | 698 | 503 | 855 | 828 | 1163 | 739 | 780 |

1. **CONCLUSION**

In this article, we have proposed an algorithm to prevent Probe, DoS, Vampire, U2R attacks. The security scheme identifies attacker nodes through their malicious behavior and also minimizes the packet dropping and routing overhead. The proposed security scheme first considers nodes in the suspicious range. Nodes due to their malicious functions are defined as attackers. The proposed scheme then blocks attacker nodes after confirmation in network. For future research, this work shall be tested in different network sizes to check scalability. We will also look at preventing multiple attacks in the network simultaneously.

**REFERENCES**

1. [A. Alsumayt](https://www.computer.org/web/search?cs_search_action=advancedsearch&searchOperation=exact&search-options=dl&searchText=Albandari+Alsumayt), [J. Haggerty](https://www.computer.org/web/search?cs_search_action=advancedsearch&searchOperation=exact&search-options=dl&searchText=John+Haggerty), [A. Lotfi](https://www.computer.org/web/search?cs_search_action=advancedsearch&searchOperation=exact&search-options=dl&searchText=Ahmad+Lotfi), “Detect DoS Attack Using MrDR Method in Merging Two MANETs”, in Proceedings of the IEEE International Conference on Advanced Information Networking and Applications Workshops (WAINA), pp. 889-895, 2016.
2. J. Pullagura J.R., V. Rao, “Simulation-Based Comparison of Vampire Attacks on Traditional Manet Routing Protocols”, In Information and Communication Technology for Sustainable, Springer, vol 9, pp. 978-981, 2017.
3. J. Vuorinen and P. Tetri, “Paradoxes in Information Security”, In IEEE Potentials, vol. 35, no. 5, pp. 36-39, Sept-Oct. 2016.
4. G. Folino and F. Angiulli, "Distributed Nearest Neighbor-Based Condensation of Very Large Data Sets," In IEEE Transactions on Knowledge & Data Engineering, vol. 19, no. 2, pp. 1593-1606, 2007.
5. Al-Roubaiey, T. Sheltami, A. Mahmoud, E. Shakshuki, H. Mouftah, “AACK: Adaptive Acknowledgment Intrusion Detection for MANET with Node Detection Enhancement”, in Proceedings of IEEE International Conference on Advanced Information Networking and Applications, pp. 634-640, 2010.
6. G. Vaseer, G. Ghai and P.S. Patheja, “A Novel Intrusion Detection Algorithm: An AODV Routing Protocol Study”, in Proceedings of IEEE International Symposium on Nanoelectronic and Information Systems (iNIS), pp. 111-116, 2017.
7. [R. Shrestha](https://www.computer.org/web/search?cs_search_action=advancedsearch&searchOperation=exact&search-options=dl&searchText=Rakesh+Shrestha), [K.H. Han](https://www.computer.org/web/search?cs_search_action=advancedsearch&searchOperation=exact&search-options=dl&searchText=Kyong-Heon+Han), [D.Y. Choi](https://www.computer.org/web/search?cs_search_action=advancedsearch&searchOperation=exact&search-options=dl&searchText=Dong-You+Choi), [S.J. Han](https://www.computer.org/web/search?cs_search_action=advancedsearch&searchOperation=exact&search-options=dl&searchText=Seung-Jo+Han), “A Novel Cross Layer Intrusion Detection System in MANET”, in Proceedings of IEEEInternational Conference onAdvanced Information Networking and Applications (AINA) pp. 647-654, 2010.
8. Yi Gong , Yong Fang, Liang Liu, Juan Li, “Multi-agent Intrusion Detection System Using Feature Selection Approach”,  in Proceedings of IEEE International Conference onIntelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), pp. 528-531, 2014.
9. P. Johnson, “Routing Protocols for Mobile Ad-Hoc Networks- a comparative performance analysis”, In Proceedings of ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), Seatle, pp .195-206, 1999.
10. M. H. Davis and U. Lang and S. Shetye, “A Cybermodel for Privacy by Design: Building privacy protection into consumer electronics”, In IEEE Consumer Electronics Magazine, vol. 4, no. 1, pp.41-49, January 2015.
11. M.K. Denko, “A Localized Architecture for Detecting Denial of Service (DoS) Attacks in Wireless AD Hoc Networks”, In Springer Intelligence in Communication Systems. IFIP — The International Federation for Information Processing, vol 190, pp. 136-146, 2005.
12. S. Ganapathy, P. Yogesh, A. Kannan, “An Intelligent Intrusion Detection System for Mobile Ad-Hoc Networks Using Classification Techniques”, In Springer Advances in Power Electronics and Instrumentation Engineering. Communications in Computer and Information Science, vol 148. pp. 117-122, Berlin, 2011.
13. P. S. Hiremath, Anuradha T, P. Pattan., "Adaptive fuzzy inference system for detection and prevention of cooperative black hole attack in MANETs", 2016 International Conference on Information Science (ICIS), 2016.
14. S. R. Das, E. M. Belding-Royer, and C. E. Perkins, “Ad hoc on-demand distance vector (aodv) routing,” 2003.

**ABOUT THE AUTHORS**

**Gurveen Vaseer** ([gurveenv@orientaluniversity.in](file:///C:\Users\Administrator\Desktop\gurveenv@orientaluniversity.in)) is a research scholar in Oriental University Indore currently pursuing research on Cyber Security since 2016. She has completed Masters of Computer Applications from RGTU Bhopal and has an experience of 11 years in the field of teaching.

**Garima Ghai** ([garimaghai@orientaluniversity.in](mailto:garimaghai@orientaluniversity.in)) is as Professor in the Department of Computer Science and Engineering at Oriental University Indore. She obtained her Ph.D. and Master of Science degree in Computer Science and Engineering from University of North Texas, USA in 2010 and 2006. She is an author/co-author of a dozen of peer-reviewed journal articles and conference publications in the disciplines of Computer Science and Electronics Engineering.

**Pushpinder Singh Patheja**([pspatheja@gmail.com](file:///C:\Users\Administrator\Desktop\pspatheja@gmail.com)) is presently working as Director, Students Welfare and Associate Professor in School of Computing Science Engineering at Vellore Institute of Technology (VIT) Bhopal Campus. He received the Ph.D. degree from Maulana Azad National Institute of Technology (NIT), Bhopal.

**Dhruva Ghai** ([dhruvaghai@orientaluniversity.in](mailto:dhruvaghai@orientaluniversity.in)) is a Professor with the Department of Electronics and Communication Engineering, Oriental University, Indore, India. He received the Ph.D. degree in computer science and engineering from the University of North Texas, USA, in 2009. He has authored 21 research papers and one book chapter in the area of VLSI and low power design and has over 200 citations. He is a Senior Member of IEEE.