TWIN-NODE NEIGHBOUR ATTACK ON AODV BASED WIRELESS AD HOC NETWORK

Alok Singh, Saurabh Sharma and Rajneesh Kumar Srivastava

Department of Electronics & Communication, University of Allahabad, India

ABSTRACT

As security is a very challenging issue in ad hoc networks, variety of research works related to security of ad hoc networks are being reported for last many years. In the present work, we propose a new sort of attack titled Twin-Node Neighbour Attack (TNNA), wherein two malicious nodes in close vicinity of each other exploits the provision of broadcast nature of Hello Messages in AODV routing protocol along with non-provision of any restriction regarding authentication of participating nodes. Mitigation measures are designed to lessen or perhaps remove security flaws and threats altogether. Detection and mitigation of TNNA attack are also proposed and discussed. The network's performance has been measured using four metrics viz. Packet Delivery Ratio, Throughput, Total Number of Received Packets and Average End-to-End Delay. It is evident from simulations that the TNNA attack is significantly detrimental to the performance of WANETs using AODV routing protocol. After attack throughput of legitimate flow is found to be less than 5 % as compared to the Throughput without attack, when the data rate of malicious node is 100 Kibps. Due to stress of malicious flow of 100 Kibps, the number of transmitted (received) data packets of legitimate flow is reduced by a factor of more than 20.

KEYWORDS

Ad Hoc Network, AODV, Neighbour Attack, NS-3.

1. INTRODUCTION

Security is a critical component of all wired and wireless communication networks. The security of a wireless ad hoc network (WANET) determines its success. The properties of WANET, on the other hand, present both obstacles and opportunities in terms of meeting security objectives such as authentication, confidentiality, availability, integrity, non-repudiation, and access control, among others.

A wireless ad hoc network (WANETs) is an independent system of mobile nodes connected by wireless links. Each node serves as both a router and an end-system for packet forwarding. The nodes are free to move around and form a network independently. The use of WANETs does not necessitate the use of fixed infrastructure such as base stations, making it an appealing networking option for connecting mobile devices quickly and spontaneously, such as in personal electronic device networking, military applications, emergent operations, and civilian applications such as an ad hoc classroom or an ad hoc meeting room [1].

Wireless ad hoc networks have various distinguishing features, including dynamic topologies, variable capacity links, bandwidth-constrained, limited physical security and energy-constrained operation. Because of these features, wireless ad hoc networks are especially vulnerable to attacks initiated from a compromised node [1].

WANETs are vulnerable to various attacks because of insecure protocols and vulnerabilities such as restricted bandwidth, dynamically changing topology, wireless connectivity, no established boundaries, and limited battery life [2].

In the present work, we propose a new sort of attack titled Twin-Node Neighbour Attack (TNNA) and the objective of the present work is as follows:

- To design and implement a new type of attack using the AODV routing protocol.
- To design and implement detection and mitigation mechanisms for this new type of attack.

In Proposed TNNA attack, where two malicious nodes in close vicinity of each other exploit the broadcast nature of Hello Messages in AODV routing protocol along with non-provision of any restriction regarding authentication of participating nodes. Mitigation measures are designed to lessen or perhaps remove security flaws and threats altogether. Detection and mitigation of TNNA attacks are also proposed and discussed. The network's performance has been measured using four metrics: Packet Delivery Ratio, Throughput, Total Number of Received Packets and Average End-to-End Delay. It is evident from simulations that the TNNA attack is significantly detrimental to the performance of WANETs using AODV routing protocol. Main contributions of this work are as follows:

- It is perhaps a new type of attack on AODV-based WANETs.
- This work presents a method also to detect and mitigate the proposed attack.

The paper is organized as follows. Literatures has been discussed in section 2. Twin-Node Neighbour Attack is discussed in section 3. In section 4, proposed algorithms of TNNA attack, its detection and mitigation have been provided. Simulation parameters and performance metrics have been presented in section 5. Results and analysis are provided in section 6. Finally, in section 7, the conclusion and future work are discussed.

2. LITERATURE REVIEW

There are a variety of attacks for WANETs, e.g., Blackhole attack, Grey hole attack, Wormhole attack, Sinkhole attack, Flooding attack, Eavesdropping attack, DoS attacks, Man-In-The-Middle [3][4][5][6][7][8][9][10][11][12][13][14][15][16][17][18][19][20][21][22][23][24][25][26][27] wherein either all packets are made to be routed to the malicious node which drops all packets or malicious nodes drop packet selectively or malicious nodes modify packets, forward packets out of order or notify neighbours that it has a low-cost route to a destination etc.

As far as AODV routing protocol is concerned, provision of identification of neighbours through exchange of Hello messages seems to be vulnerable to certain attacks. In Sinkhole attacks, a malicious node notifies its neighbours that it has a low-cost route to the destination. Neighbour nodes begin sending all packets through this node; if the node drops all packets, it becomes a Blackhole attack, depending on the implementation [12][13][14].

Goel et al. [28] offered a solution for secure transmission throughout the network, in addition to proposing a neighbour node analysis approach to identify wormhole attacks and eliminate wormhole links in MANET. The work they had shown was simulated with NS-2, and specific characteristics like loss rate, throughput, and delay rate were used to do the analysis.

Parthiban S. et al. [29] have reported the neighbour attack, whose goal is to disrupt multicast routes by misleading two nodes that are actually out of communication range of each other so that they can communicate directly with each other. The join reply packet that these two nodes exchange if they are a part of the routing mesh will be lost because there isn't actually a link between them. Considering that the packets will eventually be lost owing to the fake links, a neighbour attacker who breaches the routing protocol does not need to get involved later in the packet dropping process.

3. Twin-Node Neighbour Attack (TNNA)

The proposed TNNA Attack, its detection and mitigation are discussed as follows:

3.1. TNNA Attack

The pair of two malicious nodes try to listen to Hello messages from legitimate nodes. Once such a Hello message is received, one of the malicious nodes starts generating data to be sent to the remaining malicious node of the pair. Any legitimate node, involved in transferring data between legitimate nodes, will start participating in transfer of data from the source malicious node to the destination malicious node as both malicious nodes are in the neighbourhood of the legitimate node. If the data rate of the source malicious node is sufficiently high, it will start eating up the resources of the legitimate node, which would otherwise be utilized in transferring data of legitimate data flows. This may lead to the unwarranted performance of ad hoc networks.

3.2. Detection and Mitigation of TNNA Attack

Every legitimate node will form a list of its neighbour nodes as well as the list of data flows between pairs of any two neighbour nodes. For every such data flow, the legitimate node will investigate whether the two nodes corresponding to the data flow experience a transition from state of neighbourhood to the state of non-neighbourhood with respect to the legitimate node simultaneously while reducing its sensitivity in steps up to a minimum level or not as shown in Table 1.

In Figure 1, n_0, n_1 and n_2 are legitimate nodes of a linear wireless ad hoc network deliberately chosen so as to bring into picture the most difficult situation wherein a node (n_1) routing a data flow between legitimate nodes (here between n_0 and n_2) is attacked by TNNA-nodes M_S and M_D staying in the neighbourhood of node n_1. Figure 2 shows the flowchart of Proposed TNNA attack.

For the example being discussed, the results of simulation experiments for detection of TNNA attack is summarized in Table 1. When M_S and M_D detect Hello messages from n_1, M_S start generating data packets destined for M_D. As M_S and M_D are in the neighbourhood of n_1, n_1 will be having a route for M_D implicitly. As a result, data from M_S to M_D will be routed through n_1 and if data rate of this data flow is sufficiently high, it will start hampering the legitimate data flow between n_0 and n_2.

Table 1. States of the neighbourhood of different nodes with respect to node 'N' for different levels of sensitivity of node 'N' while the sensitivity of other nodes remains unaltered.

S.N.	**Node**	**Sensitivity of Node 'N'**			
		-100dBm	**-90 dBm**	**-80 dBm**	**-70 dBm**
1	S	S is a neighbour node of N	S is a neighbour node of N	S is a non-neighbour node of N	S is a non-neighbour node of N
2	D	D is a neighbour node of N	D is a neighbour node of N	D is a neighbour node of N	D is a non-neighbour node of N
3	M_S	M_S is a neighbour node of N	M_S is a neighbour node of N	***M_S is a neighbour node of N**	***M_S is a non-neighbour node of N**
4	M_D	M_D is a neighbour node of N	M_D is a neighbour node of N	***M_D is a neighbour node of N**	***M_D is a non-neighbour node of N**

*This simultaneous transition of nodes M_S and M_D from being neighbour nodes of N to being non-neighbour nodes of N establishes that M_S and M_D are malicious nodes.

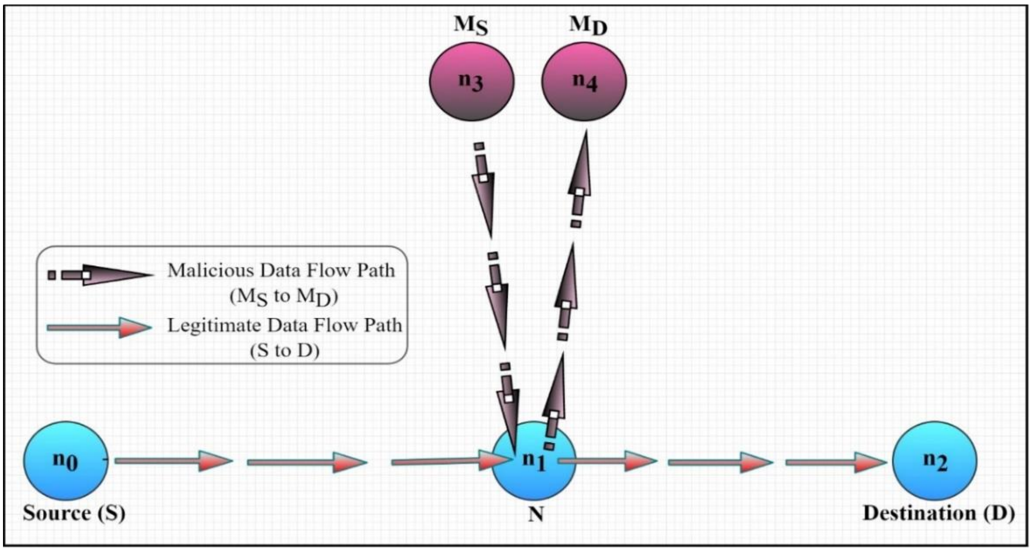


Figure 1. TNNA attack's example

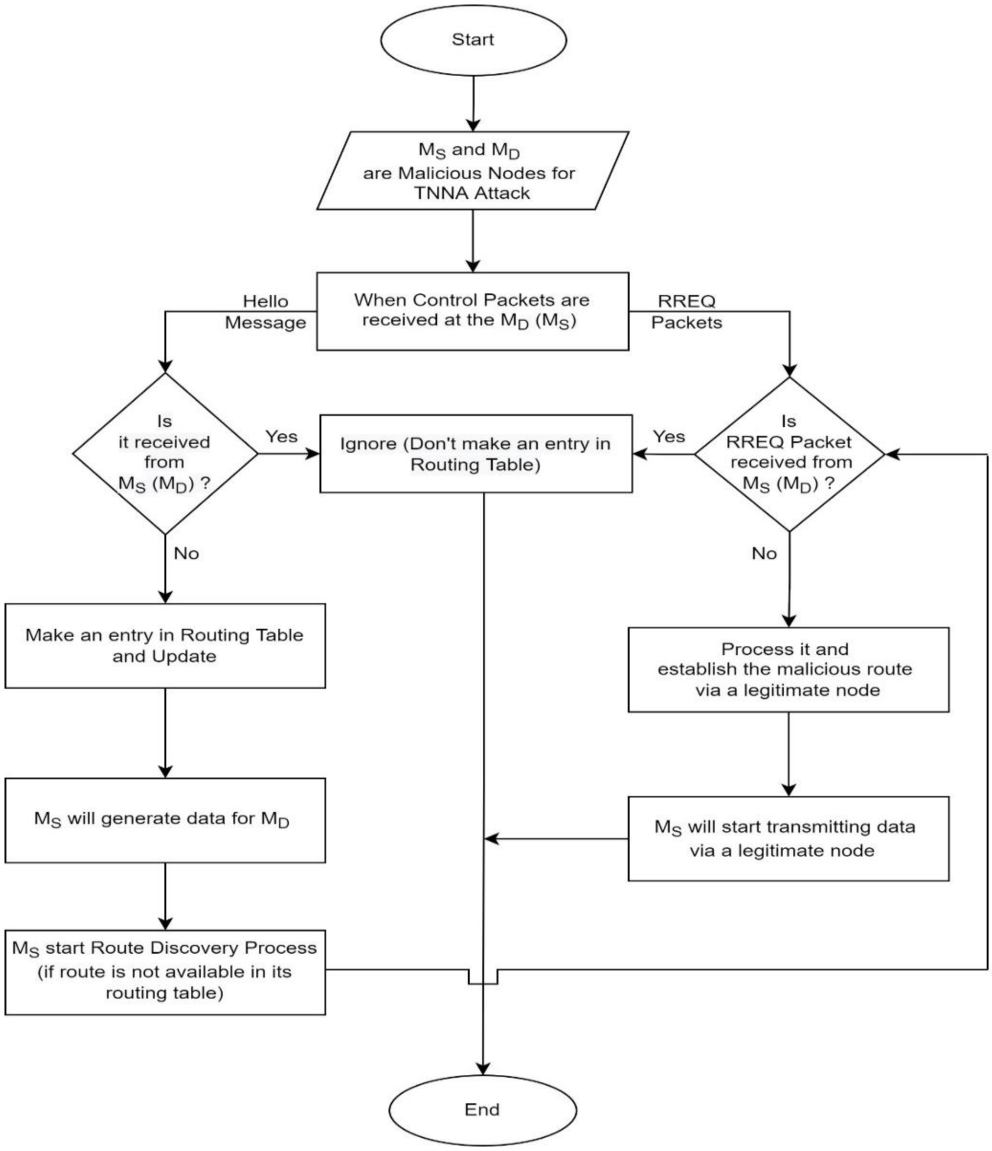


Figure 2. Flowchart of Proposed TNNA attack

4. PROPOSED ALGORITHMS OF TNNA

Symbols:

$\boldsymbol{M_p}$**:** M_p is a malicious node with identifier p.
$\boldsymbol{N_i}$: N_i is a legitimate node with identifier i.
$\boldsymbol{X(LN)}$: List of all neighbour nodes of node X.
$\boldsymbol{DF(N_S,\ N_D)}$: A data flow between source node N_S and destination node N_D exits.
$\boldsymbol{A+B}$: Node B is a neighbour node of A.
$\boldsymbol{A-B}$: Node B is a non-neighbour node of A.
$\boldsymbol{A(X[Legt])}$: State of node X is '$Legt$', i.e. node X is being treated as a legitimate node of the network by node A. This is the default state of every node.
$\boldsymbol{A(X[Susp])}$: State of node X is '$Susp$', i.e. node X is being treated by node A as a node under suspicion whether it is a legitimate node or a malicious node.
$\boldsymbol{A(X[Malc])}$: State of node X is '$Malc$', i.e. node X is being treated as a malicious node by A.

$\boldsymbol{A[X(State_i)] \rightarrow A[X(State_j)]}$: Node A changes state of node X from $State_i$ to $State_j$ where $State_i \neq State_j$ and $State_i, State_j \in \{Legt, Susp, Malc\}$.

$\boldsymbol{Sens(X)}$: Sensitivity of node X.

$\Delta\, \boldsymbol{Sens(X)}$: Step size for reduction in sensitivity of node X.

$$\boldsymbol{DFS[X(LN)]}: DF(N_p, N_q) \mid N_p, N_q \in X(LN)$$

$\boldsymbol{Sens(X)_{stop}}$: The sensitivity of X is decreased in steps up to this lowest level of sensitivities of X.

Algorithm 1:	***TNNA- Malicious Nodes Implementation***
Assumption:	M_S and M_D are nodes in very close vicinity of each other to play the role of malicious node for 'TNNA' attack. M_S is source malicious node and M_D is destination malicious node.
Step 1:	Start
Step 2:	$M_S(M_D)$ ignores Hello Message from $M_D(M_S)$
Step 3:	$M_S(M_D)$ disables route updates to $M_D(M_S)$
Step 4:	$M_S(M_D)$ ignores any RREQ from $M_D(M_S)$
Step 5:	End

Algorithm 2:	***TNNA Attack***
Step 1:	Start
Step 2:	M_S and M_D tries to listen Hello Message
Step 3:	If M_S receives Hello Message from certain legitimate nodes, $M_S$starts generating data to be sent to M_D
Step 4:	End

Algorithm 3:	***Detection and Mitigation of TNNA Attack by a legitimate node 'N'***
Step 1:	Start
Step 2:	$N(LN)$ is formed $DFS[X(LN)]$ is formed
Step 3:	Select a $DF(N_p, N_q) \in DFS[X(LN)]$ $DFS[N(LN)] = DFS[N(LN)] - DF(N_p, N_q)$ GoTo Step-4.
Step 4:	$N(N_p\,[Legt]) \rightarrow N(N_p\,[Susp])$ $N(N_q\,[Legt]) \rightarrow N(N_q\,[Susp])$
Step 5:	$Sens(X) = Sens(X) - \Delta\, Sens(X)$
Step 6:	IF $N + N_p$and $N - N_q$ or $N - N_p$ and $N + N_q$ then GoTo Step-8 ELSE GoTo Step-9
Step 7:	IF $N + N_p$ AND $N + N_q$ AND $Sens(X) \geq Sens(X)_{stop}$, GoTo Step-5ELSE GoTo Step-9
Step 8:	$N(N_p\,[Susp]) \rightarrow N(N_p\,[Legt])$ $N(N_q\,[Susp]) \rightarrow N(N_q\,[Legt])$ GoTo Step-11

Step 9: $N(N_p\,[Susp]) \rightarrow N(N_p\,[Malc])$
$N(N_q\,[Susp]) \rightarrow N(N_q\,[Malc])$

Step 10: N ignores all packets from malicious nodes N_p and N_q

Step 11: IF $DFS[N(LN)] \neq \emptyset$ GoTo Step-3
ELSE GoTo Step-12

Step 12: End

5. SIMULATION PARAMETERS

Figure 3 shows the time windows for the simulation and the On-Off Application of legitimate and malicious nodes used in our program. For the simulation experiment, we have chosen the NS-3 version 3.36.1 as the network simulator and set the seed value equal to 1 (default value) with only 1 run (number of iterations). The "On-Off Application" has been chosen for generating Constant Bit Rate (CBR) type traffic, with a packet size of 512 bytes for both malicious and non-malicious nodes. Table 2 shows other major simulation parameters with their values.

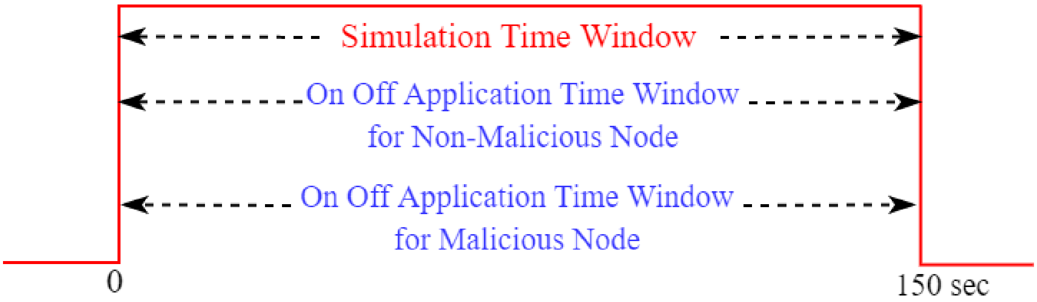


Figure 3. Different time windows

Table 2. Simulation Parameters

Parameter	Value
NS-3 Version	3.36.1
Seed	1
Run (Number of iterations)	1
Number of Nodes	5
Application	On-Off Application
	Data Rate of non-malicious source node - 20 Kib/s
	Data Rate of malicious source node – 10, 20, 30, 40, 50, 60, 70, 80, 90 and 100 Kib/s
Traffic	CBR
Packet Size (Payload)	Malicious and non-malicious source nodes = 512 Bytes
Transport Layer Protocol	UDP
Routing protocol	AODV Routing Protocol
MAC Mode	Ad-hoc
Physical Standard	IEEE 802.11b (DSSS 1 Mbps)
Propagation Delay Model	Constant Speed Propagation Delay Model

Propagation Loss Model	Log Distance Propagation Loss Model
Reference Loss	40.0459 dBm
Simulation Time	150 sec

Note: The source codes of TNNA attack, its detection and mitigation are available on GitHub [30].

5.1. Performance Metrics

The following metrics have been used to investigate the effect of TNNA attack on the performance of the ad hoc network:

5.1.1. Packet Delivery Ratio (PDR)

PDR is defined as the ratio of the total number of received data packets to the total number of transmitted data packets [31].

$$PDR = \frac{Total\ Number\ of\ Received\ Data\ Packets}{Total\ Number\ of\ Transmitted\ Data\ Packets} * 100$$

5.1.2. Throughput

Throughput is the ratio of total bits of received data packets to the simulation time. To obtain the Throughput in Kib/s, it is divided by 1024 [32].

$$Throughput\ (Kibps) = \frac{Total\ Number\ of\ Received\ Data\ Packets\ in\ bits}{(Simulation\ Time) * 1024}$$

5.1.3. Average End-to-End Delay (AEED)

is defined as the ratio of the sum of all delays experienced by delivered data packets to the total number of received data packets by the destinations [31].

$$Average\ End - to - End\ Delay = \frac{Sum\ of\ All\ Delays\ Experienced\ by\ Delivered\ Data\ Packets}{Total\ Number\ of\ Received\ Data\ Packets}$$

6. Results and Analysis

Variation of the Total Number of Received Packets, PDR and Throughput for different data rates between M_S and M_D are shown in Figure 4, Figure 5 and Figure 6 respectively. From all these figures, it is evident that at a high data rate between M_S and M_D, the performance of WANET is degraded significantly under TNNA attack if no mitigation mechanism is provisioned. However, if the provisions of detection and mitigation mechanisms are in place, the performance of the WANET is restored completely.

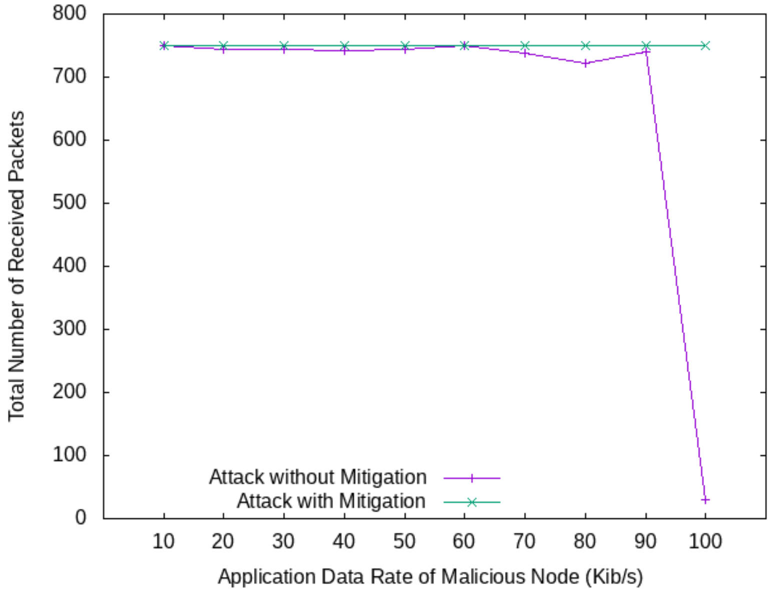


Figure 4. Variation of Total Number of Received Packets with Data Rate of Malicious Node

It is worth mentioning here that, though Throughput is usually defined as the total number of packets (bits) delivered divided by the time difference between the instant of reception of last packet and that of transmission of first packet, the co-authors resorted to the definition of Throughput as total number of delivered packets divided by the simulation time. To differentiate it, Throughput(Usual) takes into account the time difference between the instant of reception oflast packet and that of transmission of first packet whereas Throughput as defined in the present work, takes into account the simulation time.

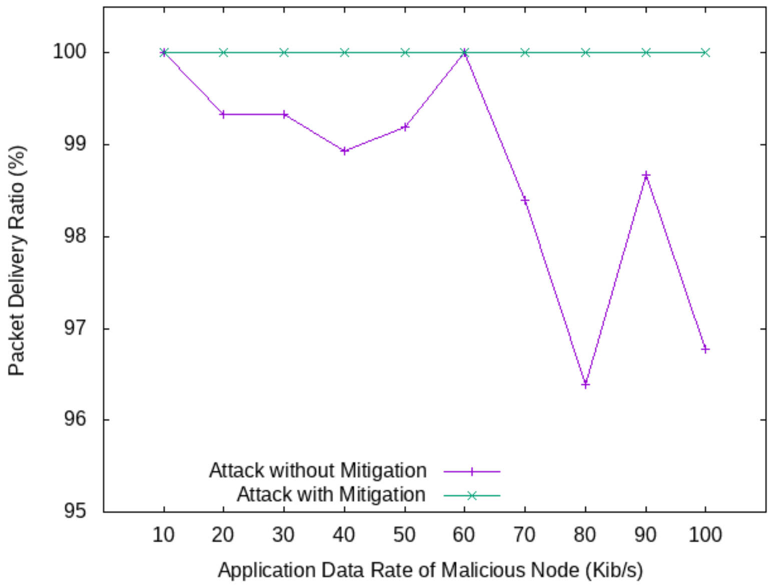


Figure 5. Variation of Packet Delivery Ratio with Data Rate of Malicious Node

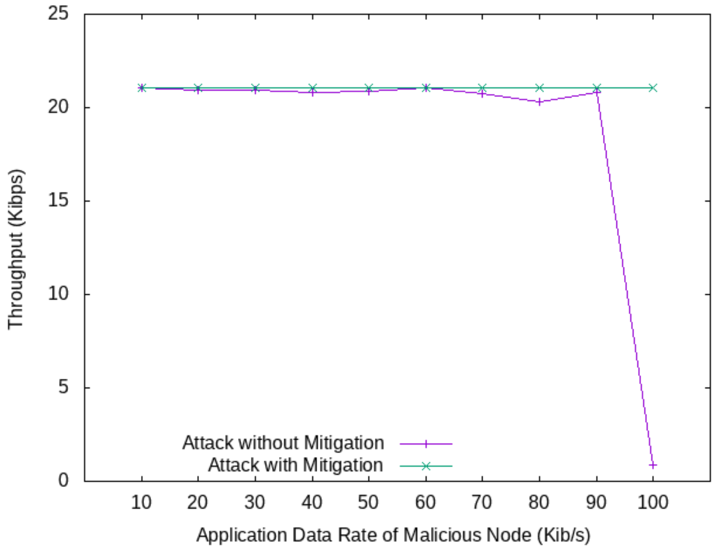
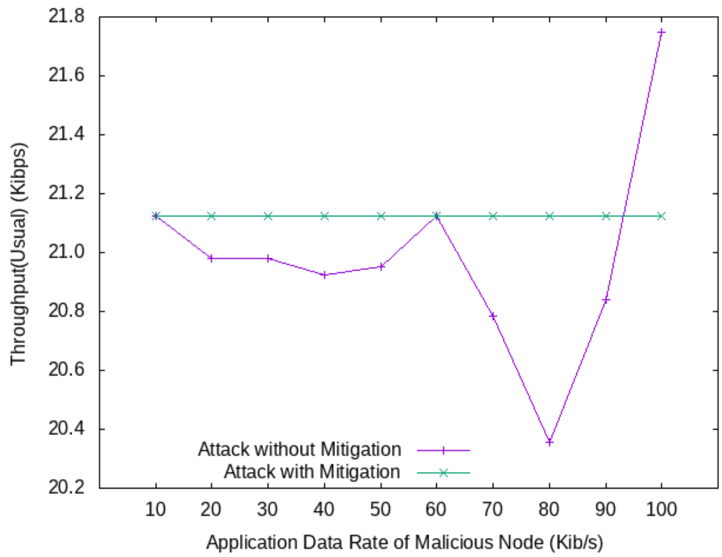


Figure 6. Variation of Throughput with Data Rate of Malicious Node

Figure 7 shows the variation of Throughput(Usual) with varying data rates between M_S and M_D. The graph is certainly not easily comprehensible. The reason could be understood by observing the last row of Table 3, wherein it could be noticed that though the number of packets generated by ‘S’ is still 749 but the number of packets transmitted by S is merely 31, and the number of received packets by ‘D' is 30. This may be attributed to the fact that at such a high data rate at which M_S is generating packets, node n_1 is so engaged in transporting data between M_S and M_D, that S is comparatively getting lesser chance of forwarding its packets to n_1.

Table 3. Number of Received and Transmitted Data Packets in presence of TNNA attack**

S.N.	Application Data Rate of Malicious Node 'M_S' (Kibps)	Number of Packets Generated by Source Node 'S'	TNNA Attack without Mitigation		TNNA Attack with Mitigation	
			Number of Packets transmitted by Source Node 'S'	Number of Packets Received by Destination Node 'D'	Number of Packets transmitted by Source Node 'S'	Number of Packets Received by Destination Node 'D'
1	10	749	749	749	749	749
2	20	749	749	744	749	749
3	30	749	749	744	749	749
4	40	749	749	741	749	749
5	50	749	749	743	749	749
6	60	749	749	749	749	749
7	70	749	749	737	749	749
8	80	749	749	722	749	749
9	90	749	749	737	749	749
10	100	749	**31**	**30**	749	749



**In absence of TNNA attack, the number of received packets by destination node 'D' is 749.

Figure 7. Variation of Throughput(Usual) with Data Rate of Malicious Node

At first glance, the Throughput (usual) is expected to be significantly low. On the contrary, it comes out to be high. Detailed investigation of events logged in ASCII Trace files reveals that at high data rate of 100 Kibps at which M_S is generating packets, the time difference between instant of reception of last packet and that of transmission of the first packet comes out as 5.82

seconds which is much lower than such time difference for the lower data rate of generation of packets by M_S which is very much close to 150 seconds. This anomaly becomes non-existent when Throughput is computed as defined in the present work.

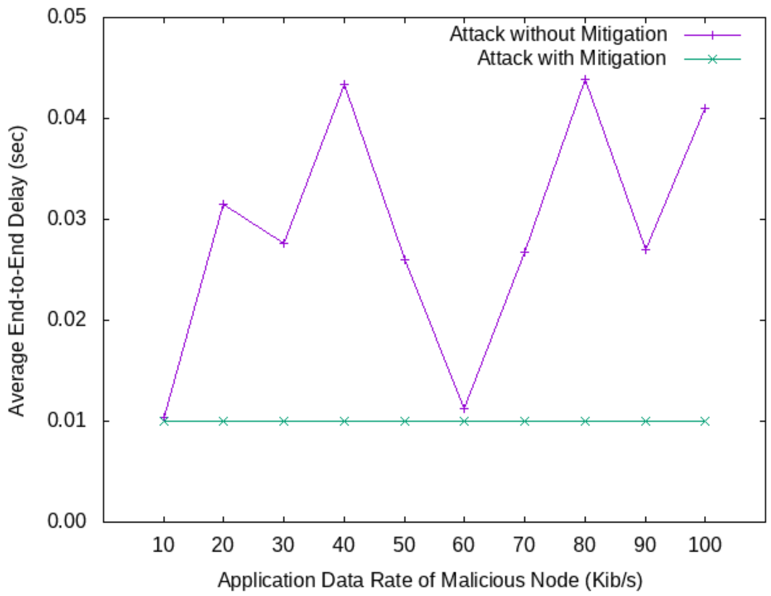


Figure 8. Variation of Average End-to-End Delay with Data Rate of Malicious Node

Variation of average end-to-end delay with data rate of malicious node is shown in Figure 8. AEED of linear ad hoc network using mitigation is lower as compared to the case with attack without mitigation. During attack the node n_1 remains engaged in routing of data packets from legitimate node n1 as well as that from malicious node M_1.

Table 4 displays the metrics obtained from the simulation when the malicious node attacked with a data rate of 100 Kib/s.

Table 4. Measured value of Metrics at 100 Kib/s data rate of Malicious node

S.N.	**Metrics**	**TNNA Attack without Mitigation**	**TNNA Attack with Mitigation**
1	Total Number of Received Packets	30	749
2	Packet Delivery Ratio (PDR)	96.7742	100
3	Throughput	0.84375 Kib/s	21.0656 Kib/s
4	Average End-to-End Delay	0.0410054 sec	0.0100343 sec

7. Conclusion and Future Work

The proposed TNNA attack is found detrimental at high data generation rate of malicious source node as far as the performance of the WANETs is concerned. The proposed detection and mitigation mechanisms are found effective to counter such TNNA attacks. After attack throughput of legitimate flow is found to be less than 5 % as compared to the Throughput without attack, when the data rate of malicious node is 100 Kibps. Due to stress of malicious flow of 100 Kibps, the number of transmitted (received) data packets of legitimate flow is reduced by a factor of more than 20.

The findings of the work is based on simulations only for a very trivial ad hoc network so it is hard to predict the impact of TNNA attack in a real ad hoc network. However, in future, TNNA attack is planned to be more devastating by making provision of many pairs of malicious nodes coordinating with each other.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] S. Sharmila and T. Shanthi, "A survey on wireless ad hoc network: Issues and implementation," *1st Int. Conf. Emerg. Trends Eng. Technol. Sci. ICETETS 2016 - Proc.*, Oct. 2016, doi: 10.1109/ICETETS.2016.7603071.

[2] M.-L. Chiang, H.-C. Hsieh, C.-F. Hsieh, W.-L. Lin, and X.-Z. Lin, "Relative Complement Set Based For Connected Dominating Set Algorithm For the Ad Hoc Network," 2021, doi: 10.21203/rs.3.rs-993551/v1.

[3] N. Khanna and M. Sachdeva, "A comprehensive taxonomy of schemes to detect and mitigate blackhole attack and its variants in MANETs," *Comput. Sci. Rev.*, vol. 32, pp. 24–44, May 2019, doi: 10.1016/J.COSREV.2019.03.001.

[4] G. Li, Z. Yan, and Y. Fu, "A study and simulation research of blackhole attack on mobile adhoc network," *2018 IEEE Conf. Commun. Netw. Secur. CNS 2018*, Aug. 2018, doi: 10.1109/CNS.2018.8433148.

[5] A. U. Khan, R. Puree, B. K. Mohanta, and S. Chedup, "Detection and prevention of blackhole attack in AODV of MANET," *2021 IEEE Int. IOT, Electron. Mechatronics Conf. IEMTRONICS 2021 - Proc.*, Apr. 2021, doi: 10.1109/IEMTRONICS52119.2021.9422643.

[6] P. P. Ioulianou, V. G. Vassilakis, and S. F. Shahandashti, "A Trust-Based Intrusion Detection System for RPL Networks: Detecting a Combination of Rank and Blackhole Attacks," *J. Cybersecurity Priv. 2022, Vol. 2, Pages 124-153*, vol. 2, no. 1, pp. 124–153, Mar. 2022, doi: 10.3390/JCP2010009.

[7] D. Dong, M. Li, Y. Liu, X. Y. Li, and X. Liao, "Topological detection on wormholes in wireless ad hoc and sensor networks," *Proc. - Int. Conf. Netw. Protoc. ICNP*, pp. 314–323, 2009, doi: 10.1109/ICNP.2009.5339673.

[8] O. R. Ahutu and H. El-Ocla, "Centralized Routing Protocol for Detecting Wormhole Attacks in Wireless Sensor Networks," *IEEE Access*, vol. 8, pp. 63270–63282, 2020, doi: 10.1109/ACCESS.2020.2983438.

[9] Y. C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks," *Proc. - IEEE INFOCOM*, vol. 3, pp. 1976–1986, 2003, doi: 10.1109/INFCOM.2003.1209219.

[10] S. K. Jangir and N. Hemrajani, "A comprehensive review on detection of wormhole attack in MANET," *Proc. 2016 Int. Conf. ICT Business, Ind. Gov. ICTBIG 2016*, Apr. 2017, doi: 10.1109/ICTBIG.2016.7892688.

[11] Y. C. Hu and A. Perrig, "Wormhole attacks in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 370–379, Feb. 2006, doi: 10.1109/JSAC.2005.861394.

[12] E. C. H. Ngai, J. Liu, and M. R. Lyu, "On the intruder detection for sinkhole attack in wireless sensor networks," *IEEE Int. Conf. Commun.*, vol. 8, pp. 3383–3389, 2006, doi: 10.1109/ICC.2006.255595.

[13] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, "Designing Efficient Sinkhole Attack Detection Mechanism in Edge-Based IoT Deployment," *Sensors 2020, Vol. 20, Page 1300*, vol. 20, no. 5, p. 1300, Feb. 2020, doi: 10.3390/S20051300.

[14] P. Bhale, S. Dey, S. Biswas, and S. Nandi, "Energy Efficient Approach to Detect Sinkhole Attack Using Roving IDS in 6LoWPAN Network," *Commun. Comput. Inf. Sci.*, vol. 1139 CCIS, pp. 187–207, 2020, doi: 10.1007/978-3-030-37484-6_11.

[15] P. Goyal, S. Batra, and A. Singh, "A Literature Review of Security Attack in Mobile Ad-hoc Networks," *Int. J. Comput. Appl.*, vol. 9, no. 11, pp. 11–15, Nov. 2010, doi: 10.5120/1439-1947.

[16] A. Bandyopadhyay, S. Vuppala, and P. Choudhury, "A simulation analysis of flooding attack in MANET using NS-3," *2011 2nd Int. Conf. Wirel. Commun. Veh. Technol. Inf. Theory Aerosp. Electron. Syst. Technol. Wirel. VITAE 2011*, 2011, doi: 10.1109/WIRELESSVITAE.2011.5940916.

[17] P. Yi, Y. Hou, Y. Zhong, S. Zhang, and Z. Dai, “Flooding attack and defence in Ad hoc networks,” *J. Syst. Eng. Electron.*, vol. 17, no. 2, pp. 410–416, 2006, doi: 10.1016/S1004-4132(06)60070-4.

[18] B. Wu, J. Chen, J. Wu, and M. Cardei, “A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks,” *Wirel. Netw. Secur.*, pp. 103–135, Dec. 2007, doi: 10.1007/978-0-387-33112-6_5.

[19] W. Yang, Z. Zheng, G. Chen, Y. Tang, and X. Wang, “Security analysis of a distributed networked system under eavesdropping attacks,” *IEEE Trans. Circuits Syst. II Express Briefs*, vol. 67, no. 7, pp. 1254–1258, Jul. 2020, doi: 10.1109/TCSII.2019.2928558.

[20] A. Vashist, A. Keats, S. M. P. Dinakarrao, and A. Ganguly, “Securing a Wireless Network-on-Chip against Jamming-Based Denial-of-Service and Eavesdropping Attacks,” *IEEE Trans. Very Large Scale Integr. Syst.*, vol. 27, no. 12, pp. 2781–2791, Dec. 2019, doi: 10.1109/TVLSI.2019.2928960.

[21] A. Nadeem and M. Howarth, “Adaptive intrusion detection and prevention of denial of service attacks in MANETs,” *Proc. 2009 ACM Int. Wirel. Commun. Mob. Comput. Conf. IWCMC 2009*, pp. 926–930, 2009, doi: 10.1145/1582379.1582581.

[22] K. Elleithy, D. Blagovic, W. Cheng, and P. Sideleau, “Denial of Service Attack Techniques: Analysis, Implementation and Comparison,” *Sch. Comput. Sci. Eng. Fac. Publ.*, Jan. 2005, Accessed: Apr. 25, 2022. [Online]. Available: https://digitalcommons.sacredheart.edu/computersci_fac/52

[23] X. Wu and D. K. Y. Yau, “Mitigating denial-of-service attacks in MANET by distributed packet filtering: A game-theoretic approach,” *Proc. 2nd ACM Symp. Information, Comput. Commun. Secur. ASIACCS ’07*, pp. 365–367, 2007, doi: 10.1145/1229285.1229329.

[24] S. Gurung and S. Chauhan, “Performance analysis of black-hole attack mitigation protocols under gray-hole attacks in MANET,” *Wirel. Networks*, vol. 25, no. 3, pp. 975–988, Apr. 2019, doi: 10.1007/S11276-017-1639-2/TABLES/7.

[25] P. Rani, Kavita, S. Verma, and G. N. Nguyen, “Mitigation of Black Hole and Gray Hole Attack Using Swarm Inspired Algorithm with Artificial Neural Network,” *IEEE Access*, vol. 8, pp. 121755–121764, 2020, doi: 10.1109/ACCESS.2020.3004692.

[26] M. Conti, N. Dragoni, and V. Lesyk, “A Survey of Man in the Middle Attacks,” *IEEE Commun. Surv. Tutorials*, vol. 18, no. 3, pp. 2027–2051, Jul. 2016, doi: 10.1109/COMST.2016.2548426.

[27] F. Ahmad, A. Adnane, V. N. L. Franqueira, F. Kurugollu, and L. Liu, “Man-In-The-Middle Attacks in Vehicular Ad-Hoc Networks: Evaluating the Impact of Attackers’ Strategies,” *Sensors 2018, Vol. 18, Page 4040*, vol. 18, no. 11, p. 4040, Nov. 2018, doi: 10.3390/S18114040.

[28] S. Goyal and H. Rohil, “Securing MANET against Wormhole Attack using Neighbor Node Analysis,” *Int. J. Comput. Appl.*, vol. 81, no. 18, pp. 44–48, Nov. 2013, doi: 10.5120/14227-2478.

[29] S. Parthiban, A. Amuthan, Ks. Joseph, and S. Tech Asst, “NEIGHBOR ATTACK AND DETECTION MECHANISM IN MOBILE AD-HOC NETWORKS,” *Adv. Comput. An Int. J. (ACIJ)*, vol. 3, no. 2, 2012, doi: 10.5121/acij.2012.3207.

[30] A. Singh, “alok-research/TNNA-Attack: Twin-Node Neighbour Attack, Its Detection and Mitigation,” *Github Repository*, 2022. https://github.com/alok-research/TNNA-Attack (accessed Jul. 18, 2022).

[31] S. SHARMA, A. Singh, and R. K. Srivastava, “Effect of NTT on Performance of AODV in a Linear AD HOC Network,” *Int. J. Next-Generation Comput.*, Apr. 2022, doi: 10.47164/IJNGC.V13I1.365.

[32] A. Singh, S. Sharma, and R. K. Srivastava, “Investigation of random waypoint and steady state random waypoint mobility models in NS-3 using AODV,” *J. High Speed Networks*, vol. 26, no. 4, p. pp.267-274, Dec. 2020, doi: 10.3233/JHS-200643.

AUTHORS

Mr. Alok Singh received M.Tech. Degree in Electronics and Communication Engineering (Communication System Engineering) from Sam Higginbottom Institute of Agriculture, Technology and Sciences, Prayagraj, India. He is pursuing a Ph. D. degree in the Department of Electronics & Communication, University of Allahabad, Prayagraj, India. His research interest includes Wireless Sensor Network, Wireless Ad Hoc Networks, MANET and IoT. He is a life time member of the IETE.

Mr. Saurabh Sharma received a B.Tech degree in electronics and communication engineering from UPTU Lucknow, Uttar Pradesh, India and an M.Tech degree in electronics and communication engineering from the Sam Higginbottom University of Agriculture, Technology, and Science at Prayagraj, Uttar Pradesh, India. He is pursuing Ph. D. from the department of electronics and communication, University of Allahabad, Prayagraj, Uttar Pradesh, India. His research focuses on Wireless Ad Hoc Networks, IoT, MANETs, and WSNs.

Dr. Rajneesh Kumar Srivastava received his degree of Ph. D. in 2008 from the Department of Electronics & Communication, University of Allahabad, India. He did his M. Tech. in 1999 from IIT, BHU, India. He is presently working as a Professor in the Department of Electronics & Communication, University of Allahabad, Prayagraj, India. His research interest includes Wireless Ad Hoc Networks and Photoconductivity in Nanomaterials. During his research of more than two decades, Dr Srivastava published more than 100 research papers in International Journals and Conferences. He has also served as Member (Research Staff) in Central Research Laboratory, Bharat Electronics Limited, India. He has been Honorary Secretary and Chairperson of IETE, Allahabad, India.