iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VIII **Month of publication:** August 2022

DOI: https://doi.org/10.22214/ijraset.2022.46209

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VIII August 2022- Available at www.ijraset.com

Detection and Isolating Flood Rushing Attacks in WSN Using Timer Based Trolling Technique

Deeksha Sahu[1], Mr. Rajneesh Pachouri[2], Mr. Anurag Jain[3]
[1, 2, 3]*Department of computer science and engineering AIST, Sagar (M.P.)*

Abstract: ***The Mobile Ad hoc Network (MANET) is a wireless network component that offers a variety of applications in numerous industries. Perhaps the biggest problem with networks was the security of MANET. MANET is defenceless against many attacks that affect its availability and functionality. The black hole attack is one of the most dangerous dynamic assaults since it prevents the network from being presented and reliable because the malicious node drops all incoming data packets. By ensuring that it always has the best path to the target node, the black hole attack aims to trick every node in the network that wants to communicate with another node. A black hole attack into the network cannot be detected or prevented by the responsive routing protocol AODV. In this study, we improved the AODV routing protocol by using a different, more lightweight technique that recognises and detects single and multiple black hole attacks using hop count and trolling.***
In this study, we present a security method for MANET against solitary and group black hole attacks. The blackhole attack is a packet-dropping attack that acts like a regular node during connection formation and drops all data packets after forwarding a bogus reply from the destination to the sender. With the help of other regular nodes, one or more malicious nodes in this assault establish a safe environment. The proposed IDS (Intrusion Detection System) locates nodes that are not continually forwarding data packets but are still present in the network and offers secure communication in a dynamic network.
Keywords: Blackhole, MANET, Routing, Security, IDS, Malicious nodes,

I. INTRODUCTION

Networks of Mobile ad hoc networks (MANET) are assortment of remote organizations, which comprises of immense number of versatile hubs. Hubs in networks of Mobile Ad hoc (MANET) can interface and leave the organization progressively. The portability and adaptability of MANET which doesn't need any fixed organization foundation, makes it mainstream for various applications. In this way, it is extremely helpful for crisis circumstance like military activity or calamity the executives. By methods for definition, MANET is a gathering of vagrant hubs that performing working as the transmitter and collector both speak with one another by means of bidirectional connection uncomplicatedly or in a approximately way referenced in figure 1. Through RREQ, requests are communicated by the sender, and RREP, responses are communicated back to senders by the recipient. The least bounce tally esteem determines the course of action for information transmitting. In order to deliver information in a particular organisation, the S-C-D path in the middle is chosen rather than the rest of them.

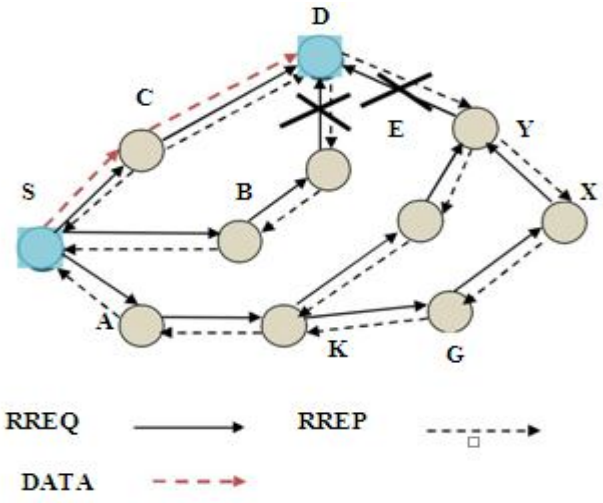


Figure 1 Mobile Ad-hoc Network

MANET is an independent, self designing organization. This organization can be conveyed anyplace easily without no help on any fixed foundation. There is foundation less and concentrated organization in this sort of organizations. Hubs are steady from first to last remote interface. Such organisations are particularly vulnerable to various connection attacks because of their dynamic design. Secure conventions that ensure tact, accessibility, validity, and organisational actuality are important requirements for a remote systems administration that is assured. Many existing wellbeing answers for wire situated organizations are inefficacious and wasteful for Mobile specially appointed organizations (MANET) climate. An impromptu organization is the co-usable climate of an arrangement of portable hubs which doesn't needed a block of any unified framework. An impromptu organization is the briefly settled and made organization, which is overseen and worked by taking interest hubs A group or collection of mobile hubs that may link to one another using multi-bounce distant connections is known as a portable specifically appointed organisation (MANET). A flexible particularly appointed organisation does not require a defined organisational geography or a uniform administration system.

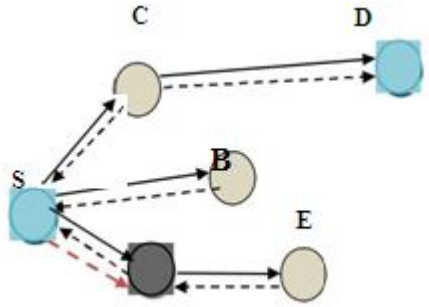


Figure 2 A Attack on Black Hole in MANET

A portable specifically appointed organisation is an independent, geographically or foundationally unrestricted, and self-managed organisation. In light of their self-foundation, self-creation, and self-maintenance, MANET is utilised widely across regions. A key component of communication for flexible framework is portable specifically designated organisation (MANET). There is a possibility to separate from or leave the mobile framework, hub, or device in the mobile spontaneous organisation. “In a blackhole assault [2,3] an assailant gets parcels from the sender and answer through bogus data of objective., and referenced in figure 1.2. The An is aggressor hub and S is sender and D is beneficiary”.

II. TECHNICAL BACKGROUND

A. Routing Strategies

Steering is the way toward finding a reasonable course for sending parcels from a source to an objective. Steering is to create solid and effective courses between pair of hubs for information transmission. To send a parcel from source to objective it could be important to jump a few bounces (multi-bounce) before a bundle arrives at the objective. To encourage the correspondence inside organization, steering convention is required. The directing convention [29] has two fundamental errands which they perform, choosing suitable and best course between the imparting hubs and the upkeep of courses for conveyance of messages to their right objective. The course to be trailed by the bundles is controlled by the organization layer. The calculations used to ascertain these courses are known as directing calculations. Traditionally all the steering conventions depend on one or other of the accompanying directing methodologies. Directing techniques followed by the steering conventions depend on calculations that the hub (either has or switches) follows to advance information parcels.

B. Distance Vector Routing

Distance-vector alludes to a class of calculations used to spread directing data. In distance vector steering every hub screens the expense of its active connections as it were. All in all, every hub screens the course to its straightforwardly associated neighbors [30, 31]. Hubs at that point intermittently broadcast to every one of its neighbors a gauge of the most brief distance to each other hub in the organization.

The getting hubs compute the following jump for every objective by contrasting the distances got from different hubs utilizing a most brief way calculation and spare it in directing tables. Hence the steering tables of distance vector based directing conventions contain course sections for all the known objections in the organization. All the hubs intermittently share a duplicate of their directing table with their neighbors.

Distance vector calculations are anything but difficult to actualize. Not with standing, distance vector directing experiences moderate combination and circle arrangement. The essential driver for this is that the hubs pick their next-jumps in a totally conveyed way dependent on data that might be old and invalid.

C. *Flooding*

Many routing protocols uses broadcast to exchange and share control information. A node sends the control information to all other nodes in the network. Another form of broadcasting is flooding in which each node sends its information to its neighbours. The neighbours relay this information to their neighbours and so on, until the packet has reached all nodes in the network. A node relays packet only once and to make sure that this sequence number may not be further used, when a node relays a new packet it increment the sequence number by one. Therefore, a node must be uniquely identified by their node id and unique sequence number.

III. PROPOSED SECURITY SCHEME AGAINST SINGLE AND MULTIPLE BLACKHOLE ATTACK

A. *Problem Statement*

The attacker in MANET is degrades the routing performance. As we know that the behaviour of attacker are of two types. First is active attacker and other kind of attack is passive attacker. The passive attackers are not very harmful for the communication but these attackers are drop only some amount of packets in network. The active attacker is very harmful for communication because it continuously targets the data packets in network. The blackhole attacker is active attack and their presence in network is very harmful.

The multiple attacker presence is more dangerous than single attacker presence because multiple attacker presence is cover the all normal nodes communication and drop the valuable data of senders. In MANET normal nodes are not possible to identify the blackhole attacker presence in network. The attacker presence in network is drop the data packets is huge quantity because of that the packet receiving is reduced and also the throughput performance of network is minimized. The performance of end to end TCP and UDP protocol is also affected.

B. *Proposed Security Scheme to Find and Block Blackhole Attacker*

The proposed procedure is created to oppose brilliant dark opening assaults by utilizing counter and savaging messages. The proposed procedure comprises of two stages: savaging and Nonneighbor Reply. In savaging stage every hub has a savage clock, the estimation of the clock is set haphazardly to B seconds, and each time the clock arrives at B it makes and broadcasts a savage solicitation with an arbitrarily created counterfeit id.

Contingent upon the characteristic conduct of a dark opening hub when it gets any course demand it reacts with an answer asserting that it has the best way regardless of whether it doesn't exist.

At the point when the dark opening gets the savage solicitation it sends an answer to the source hub asserting that it has a course; when the source hub gets the answer it promptly considers the hub which reacted as a dark opening and adds it to the dark opening rundown since it professed to have a course to a phony hub. In the snare demand, the estimation of TTL (Time-To-live) is set to one to try not to block the organization with counterfeit solicitations. As in a local AODV when any hub needs to speak with another in the organization it communicates RREQ to the objective hub. In Nonneighbor Reply stage every hub knows its neighboring hubs due to the welcome message broadcasting measure. At the point when the source hub gets an answer it checks the id of the base distance node(MDN) on the off chance that it is in the dark opening rundown; at that point it disposes of the answer; else it checks if the id exists in the neighbor list by contrasting the ID and ones in the neighbor list; on the off chance that MDN isn't a neighbor hub, at that point the source hub disposes of that answer to evade any correspondence with obscure hubs. The proposed procedure gives a self-discovery and segregation for any dark opening hub which empowers the network between MANET hubs. The recommended strategy doesn't utilize the dark opening caution to keep any brilliant dark opening hub from utilizing this component by communicating bogus alerts.

We set the TTL of the savage solicitation to one to try not to block the organization by savage solicitations and reactions. The arbitrariness in both phony id and savage clock will keep the dark opening hub from recognizing any example to counter this strategy. No overhead and exceptional parcels are utilized which make it a lightweight strategy.

IV. SIMULATION ENVIRONMENT

This section is the major portion of the thesis, it is important to setup simulation environment to observer protocols behavior over MANET. Quantitative analysis is conducted to with the help of NS-2 tool.

A. Network Simulator

The NS-2 (Network Simulator) [49] is the discrete event driven simulator used for implementation and the simulations of the various network protocols. It is freely distributed, open source and is widely used for the research.

NS-2 is also providing infrastructure for tracing, visualization, error models, etc. and to modify or creates your own modules. Using components in ns, many traffic and topologies can be generated and NAM (Network Animator) can be used for visual outputs.

Network simulator is the open source event driven simulator, which is basically design for simulating the communication networks such as wire oriented network, wireless ad hoc network and wireless sensor network. NS-2 (Network Simulator) contains the various module for the network such as routing, application layer protocol, transport layer protocol. Performance of network can be evaluated by researchers by configuring the network in any scripting language such as tcl and Otcl. They can get the result created by NS2. NS2 is a network simulator that is open source available, described by T and it has wide area used.

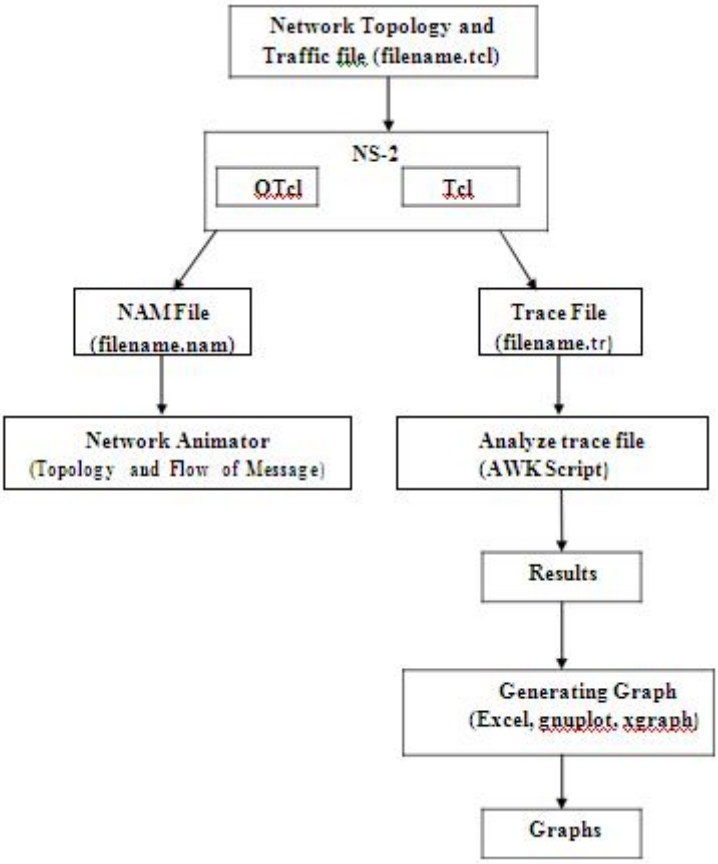


Figure 3 Simulation Procedure

B. Network Animation (NAM) Trace

The NAM trace is records of simulation detail in a text file, and uses the text file to play back simulation using the animation. NAM trace is activated by the command "$ns namtrace-all $file", where ns is the Simulator handle and file is a handle associated with the file which stores the NAM trace information. After finding a NAM trace file, the animation can be started directly at the command prompt through the following command

```
>># nam FileName.nam
```

Many visualization features are available in NAM. As animated packet flows, dropping, labelling nodes at a specified instant, shaping the nodes, coloring a link, and attacke and IDS nodes are shown in the figure 4

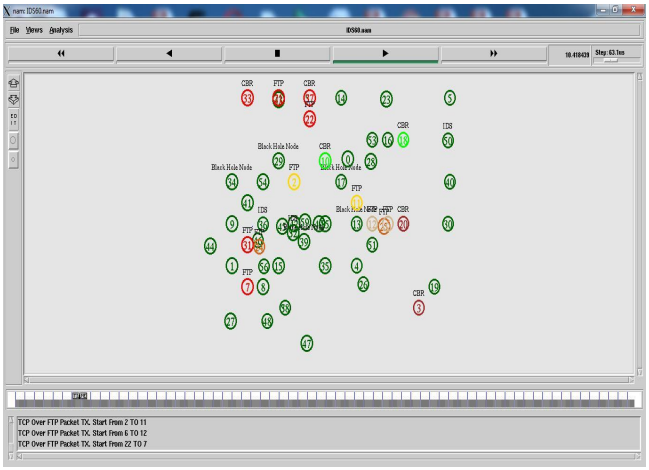


Figure 4 NAM Visualization

V. RESULT ANALYSIS

A. Simulation Results Of Single Black Hole

As appeared in Figure 3 the consequence of Throughput in local AODV when there is a dark opening hub in the organization was the most reduced in view of the bundle dropping brought about by the dark opening hub. The aftereffect of Throughput in local AODV when there is no dark opening hub in the organization was the most elevated. Taking a gander at the consequences of CBTT demonstrated a higher throughput than local AODV when there is a dark opening hub, yet lower than local AODV when there is no dark opening hub in the organization. The throughput improvement of recommended CBBT is because of dropping any answer From obscure hubs that guarantees that they have a more limited way than some other hub to the objective hub which prompts diminishing the throughput. Likewise, the situation of the dark opening hub plays a significant principle, as it very well might be situated in the most limited way between the source and objective.

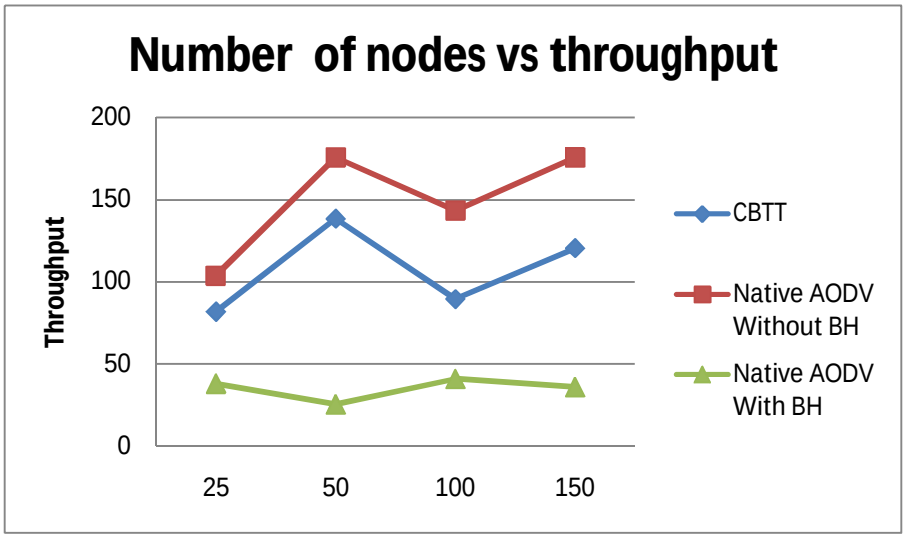


Figure 5 Results of Throughput vs. the number of nodes

As appeared in Figure 4 the aftereffect of End-to-End Delay in local AODV when there is a dark opening hub in the organization was the most elevated. The aftereffect of End-to-End Delay in local AODV when there is no dark opening hub in the organization was the most minimal in light of the AODV instrument in choosing the briefest path.The consequences of CBBT demonstrated a slight distinction in End-to-End Delay results contrasted and local AODV when there is no dark opening hub and this is a direct result of the way choice system in CBBT which stays as before as in local AODV.

Table 1Number of nodes vs. Throughput

Number of Nodes	CBTT	Native AODV Without BH	Native AODV With BH
25	80.99	102.735	37.962
50	139.137	174.236	24.544
100	88.542	142.368	40.251
150	121.5	174.689	35.248

B. Simulation Results Of Multiple Black Holes

As appeared in Figure6 the consequence of local AODV against helpful dark opening hubs demonstrated a zero Throughput because of actuality that expanding number of dark opening hubs in the organization will undoubtedly forestall the association between the source hub and the objective hub. The consequence of Throughput in CBBT AODV is diminished while expanding the quantity of dark opening hubs in the organization. The drop in Throughput is a result of the situation of the dark opening that might be situated in the way between the source hub and the objective hub, notwithstanding the way that CBBT drops any answer from obscure hubs.

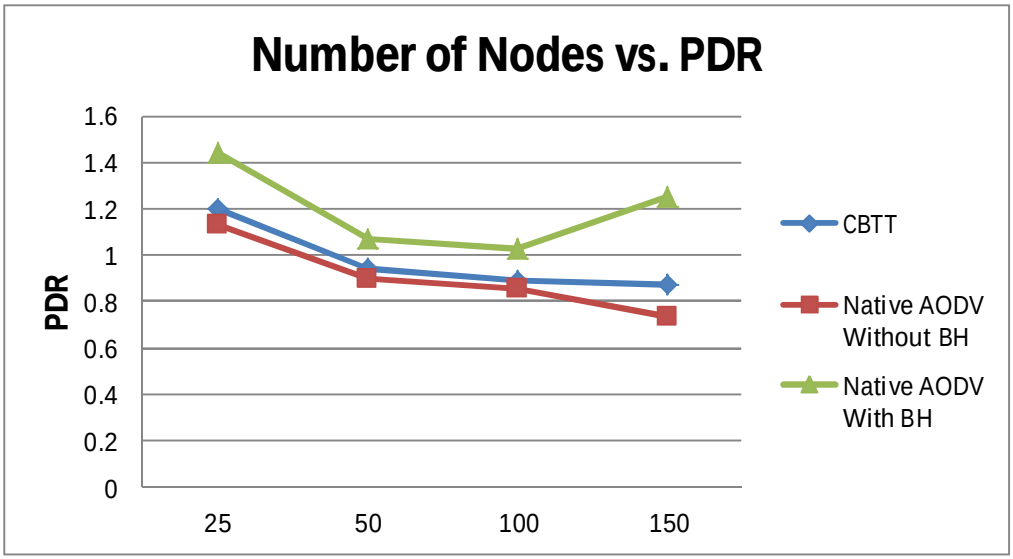


Figure 6 Results of Throughput vs. PDR

Table 2Number of BH nodes vs. Throughput

Number of Nodes	CBTT	Native AODV Without BH	Native AODV With BH
25	1.195	1.12	1.442
50	0.934	0.902	1.064
100	0.884	0.852	1.021
150	0.871	0.733	1.251

The consequence of End-to-End Delay in local AODV when there were just two dark opening hubs in the organization was the most elevated. Likewise when the quantity of dark opening hubs expanded the association between the source hub and the objective hub was forestalled so the End-to-End Delay arrived at endless. CBBT AODV demonstrated a slight distinction End-to-End Delay results with local AODV while expanding number of dark opening hubs in light of the fact that the instrument in choosing the way remains equivalent to in local AODV.

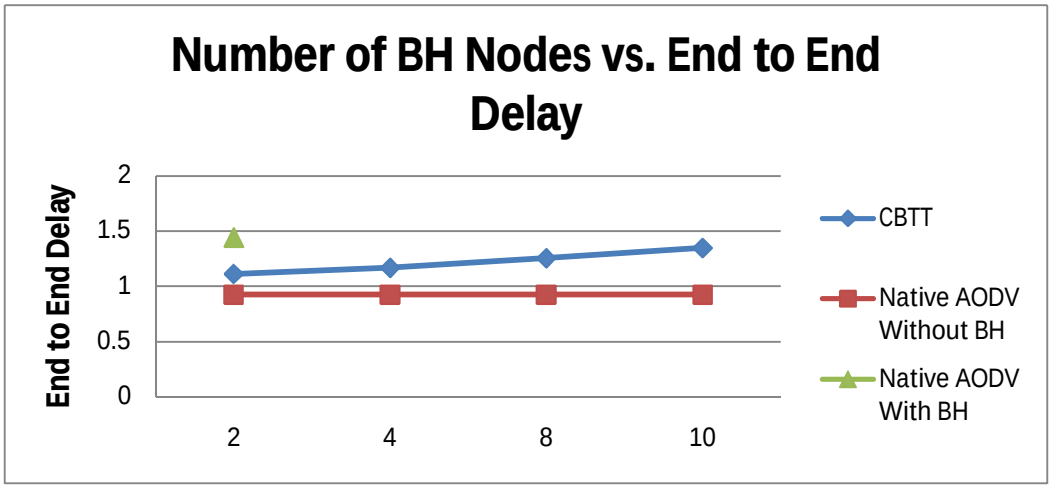


Figure 7Number of BH nodes vs. End to End Delay

Number of BH	CBTT	Native AODV Without BH	Native AODV With BH
2	1.112	0.922	1.441
4	1.164	0.922	∞
8	1.251	0.922	∞
10	1.344	0.922	∞

Figure 8 Number of BH nodes vs. End to End delay

As appeared in Figure 9 the aftereffect of local AODV against agreeable dark opening hubs indicated a zero PDR on the grounds that when the quantity of dark opening builds they will cover the entire organization, which will without a doubt cut any correspondence between any two hubs in the organization. The aftereffect of PDR in CBBT AODV is diminished while expanding the quantity of dark opening hubs in the organization. The diminishing in PDR is a result of the situation of the dark opening hubs that might be situated in the way between the source hub and the objective hub, notwithstanding the way that CBBT drops any answer from obscure hubs.

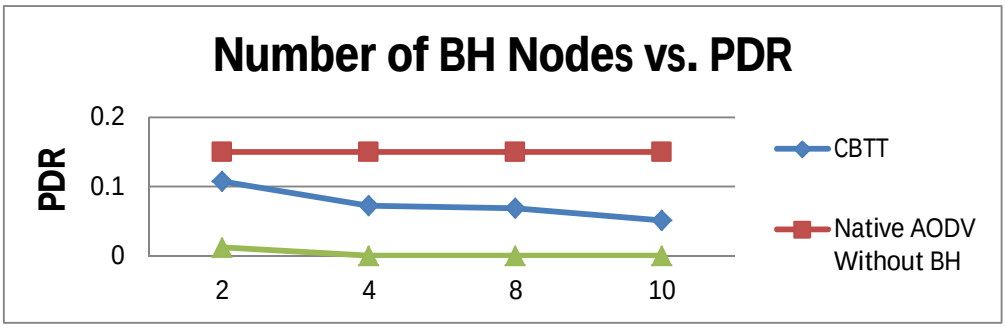


Figure 9 Number of BH nodes vs. End to PDR

Number of BH	CBTT	Native AODV Without BH	Native AODV With BH
2	0.10791	0.15039	0.01157
4	0.07316	0.15039	0
8	0.06905	0.15039	0
10	0.05121	0.15039	0

Figure 10 Number of BH nodes vs. End to PDR

VI. CONCLUSION AND FUTURE WORK

The single attacker node presence is harmful for network then the multiple blackhole effect is really more harmful for network. The same malicious function is performed by other attacker nodes by that packet dropping is improves and whole network are easily covered by attackers for injecting more infection. For improving network performance, we provides the reliable security scheme on the basis of packet dropping behavior of nodes in network. This research is very useful in field of security to evaluate the network performance in case of attack and IDS. The attack in MANET is easily loss the data and degrades the network routing performance. The previous work is provides the idea about how the different security scheme is apply the proper procedure to secure MANET routing performance.

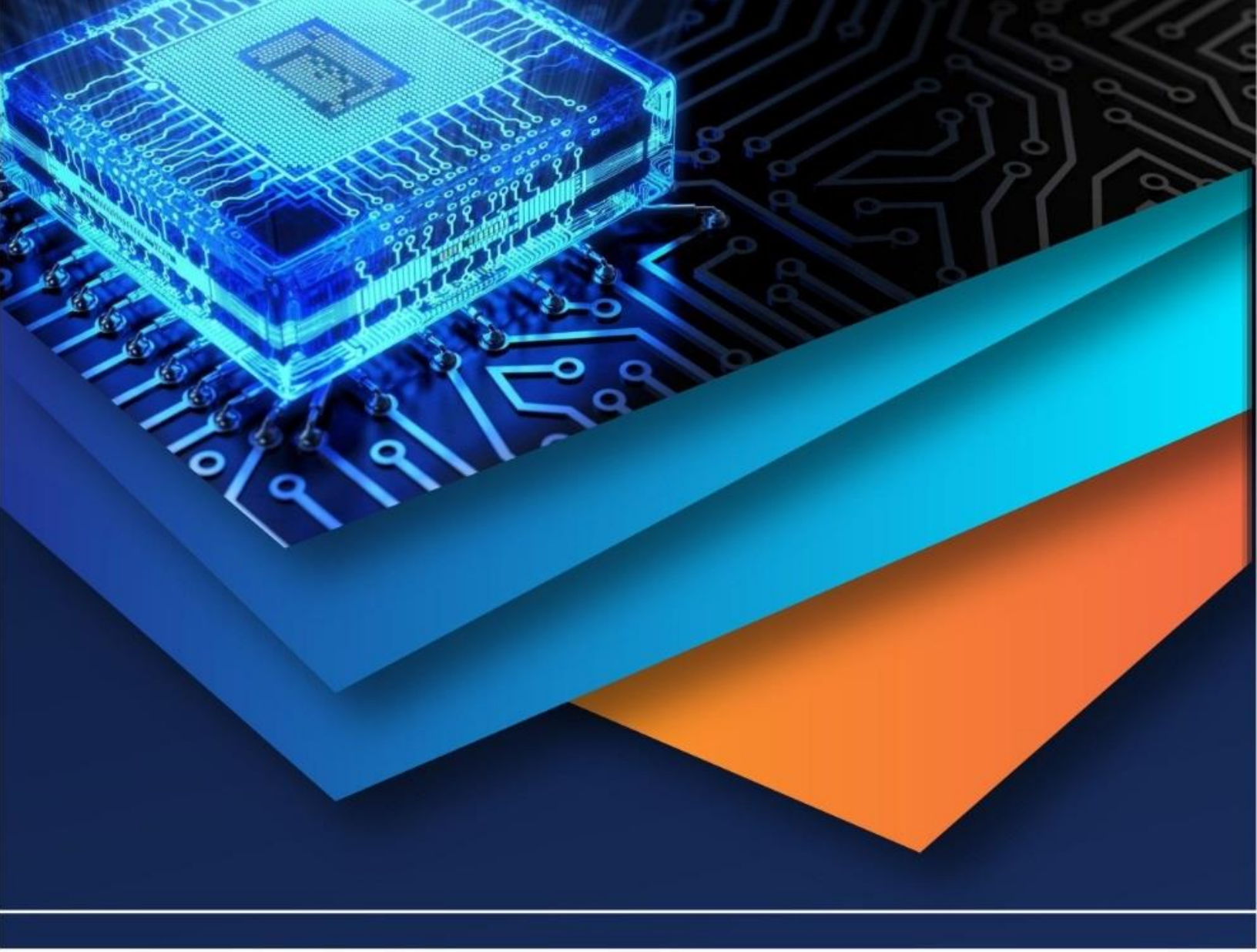
The attacker presence is loss all data of network only some data is possible to deliver in destination in particular simulation time. The proposed IDS is recognized the behavior of blackhole attack by dropping property of attacker and also their presence is one hop count distance from sender. The proposed IDS behavior is maintain consistency for watching network behavior. The number of malicious nodes quantity is also identified by same packet dropping behavior. The simulation of network is performance in 30 nodes and 60 nodes. In both the scenario attacker effect is really terrible but after applying IDS attacker effect is controlled and also blocked by IDS in network. The performance of network is improves applying proposed security scheme that improves PDR, throughput and minimizes packet dropping in network.

In this scheme the detection is based on RSS (Received Signal Strength) of mobile node and if node is drop packets then their RSS is week. Now check the reliability of node on the basis of packet dropping. The blackhole attacker is packet dropping attacker and other attacks like Tunnel attack is also the packet dropping attacker in dynamic network. In future we proposed the novel security scheme against Tunnel attack. The proposed scheme is also applied on tunnel attack in MANET.

REFERENCES

[1] C.Siva Ram Murthy and B S Manoj, „Mobile Ad Hoc Networks-Architecture and Protocols", Pearson Education, ISBN 81-317-0688-5, 2004.
[2] Yongguang Zhang and Wenke Lee, Security in Mobile Ad-Hoc Networks, in Book Ad Hoc Networks Technologies and Protocols, Springer, 2005.
[3] M. A. Shurman, S. M. Yoo, and S. Park, "Black hole attack in wireless ad hoc networks," in ACM 42nd Southeast Conference (ACMSE˝04), pp. 96-97, April. 2004.
[4] Mohd Anuar Jaafar and Zuriati Ahmad Zukarnain, "Performance Comparisons of AODV, Secure AODV and Adaptive Secure AODV Routing Protocols in Free Attack Simulation Environment", European Journal f Scientific Research, pp. 430-443, 2009.
[5] Khin Sandar Win," Analysis of Detecting Wormhole Attack in Wireless Networks", World Academy of Science, Engineering and Technology 48, pp. 422-428, 2008.
[6] Sathish, Arumugam, S.Neelavathy Pari, Harikrishnan V, "Detection of Single and Collaborative Black Hole Attack in MANET", This full-text paper was peer-reviewed and accepted to be presented at the IEEE, WiSPNET, 2016.
[7] V. Keerthika, N. Malarvizhi, "Migrating Blackhole Attack using Trust with AODV in MANET", IEEE, 2016
[8] Raquel Lacuesta, Jaime Lloret, Miguel Garcia and Lourdes Penalver, "A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation", IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No.4, 629-641, April 2013.
[9] Raj PN, Swadas PB, "DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET', International Journal of Computer Science Issue, Vol. 2, pp 54-59, 2009.
[10] Neelesh Kumar Panthi, Ilyas Khan, Vijay k. Chaudhari, "Securing Mobile Agent Using Dummy and Monitoring Mobile Agents" , "International Journal of Computer Science and Information Technologies,(IJCSIT), Vol. 1 (4) , pp. 208-211, 2010.
[11] L.Tamilselvan, Dr.V. Sankaranarayanan, "Prevention of Co-operativeBblack hole attack in MANET ", Journal of Networks,, 2008,pp. 13– 20.
[12] Sun B, Guan Y, Chen J, Pooch UW , " Detecting Black-hole Attack in Mobile Ad Hoc Networks". 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, 22-25 April 2003.
[13] Marco Fiore, Claudio Ettore Casetti, Carla-Fabiana Chiasserini, and Panagiotis Papadimitratos, "Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks ", IEEE Transactions on Mobile Computing, Vol. 12, No. 2, Pp. 289-303, February 2013

[14] X.Y. Zhang, Y. Sekiya and Y. Wakahara, “Proposal of a Method to Detect Black Hole Attack in MANETs”, Proceeding of IEEE International Symposium on Autonomous Decentralized System ISADS, 2009.
[15] Panagiotis Papadimitratos and Zygmunt J. Haas , "Secure Routing for Mobile Ad hoc Networks", In Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, pp 1-13,January 27-31, 2002
[16] K. S. Sujatha, Vydeki Dharmar, R. S. Bhuvaneswaran “Design of Genetic Algorithm based IDS for MANET”, International Conference on Recent Trends in Information Technology (ICRTIT), pp. 28-33, 2012.
[17] Dr Karim KONATE, GAYE Abdourahime “Attacks Analysis in mobile ad hoc networks: Modeling and Simulation”, 2011 Second International Conference on Intelligent Systems, Modelling and Simulation, pp. 367 – 372, 2011.
[18] N. Gandhewar, R.Patel, “Detection and Prevention of Sinkhole Attack on AODV Protocol in Mobile Adhoc Network”, Fourth International Conference on Computational Intelligence and Communication Networks (CICN), pp. 714 – 718, 2012.
[19] P.K Singh, G. Sharma, “An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET”, IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 902 – 906, 2012.
[20] Jian-Ming Chang, Po-Chun Tsou, Han-Chieh Chao, Jiann-Liang Chen, “CBDS: A Cooperative Bait Detection Scheme to prevent malicious node for MANET based on hybrid defense architecture”, 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology (Wireless VITAE), pp. 1-5, 2011.
[21] Yi Zhang, QiangLiu “A Real-Time DDoS Attack Detection and Prevention System based on per-IP Traffic Behavioral Analysis”, 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), pp. 163 – 167, 2010 .
[22] Husain. Shahnawaz, Gupta S.C., Chand Mukesh, “Denial of Service Attack in AODV & Friend Features Extraction to Design Detection ”, IEEE International Conference on Computer & Communication Technology (ICCCT), pp. 292- 297, 2011.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY