DOI: 10.21917/ijct.2021.0366

DETECTION OF BLACK HOLE ATTACK USING CROSS LAYER CONCEPT IN MANET

Shyam Sunder Karma
Department of Electronics Engineering, Dhar Polytechnic College, India

Abstract

Mobile Nodes can communicate mutually if it falls in the sensing range of the neighboring nodes. Connected nodes can transmit, receive and forward packets to connected nodes. In this paper, we focus on detection of Black Hole attack in the MANET using the cross-layer techniques that can optimize the energy consumption. The proposed cross-layer framework contains three layers and uses parameters like mobile nodes, area and the data in network layer. The MAC and data-link layer is used as a sub-layer, and a full-duplex interface is developed through the physical (PHY) layer. Our focus here is make a secure mechanism particularly to counter Black Hole Attacks through cross-layer proposal. The proposed framework is simulated using NS-3 version NS-3.17. Our examination observes the correlation between Cross Layer and Black Hole Cross-Layer scenario. This correlation is noticed between the simulation time and mobile nodes in view of the QoS parameter like execution time, redundancy gain, average end to end delay, average throughput, and network reliability. A redundancy gain performing 100% in Cross Layer with respect to Black Hole Cross Layer, thus increases the performance of the network. The simulation results show that Cross Layer approach and detection of Black Hole in Cross Layer Network is better than Black Hole Cross Layer.

Keywords:

Cross Layer, Black Hole Attack, MANET, Security

1. INTRODUCTION

The decentralized idea of the Adhoc remote systems makes them appropriate for the assortment of uses where the focal hubs can't be depended upon. It likewise enhances the versatility of remote Adhoc organizes when contrasted with remote oversaw systems. Additionally, Adhoc systems can without much of a stretch coordinate with the current framework arranged system in this manner expanding the extent of their applications [1]-[5]. Some of the applications are summarized for reference.

When a disaster happens, it is conceivable, that the communication framework may collapse totally and need to be re-establish rapidly. In such a circumstance, an especially user designed wireless system including wideband abilities can be utilized to give emergency administration. By utilizing a portable importance system, a communication system can be set up in hours rather than weeks.

Wireless designed system based on MANET for cross-layer system have applications in Mobile Ad-Hoc Network. The network concentrations on dismembering and improved the most commonly used MANET optimization control are cross- layer model based on energy consumption and throughput optimization during the attacker presence in the network. Here we have used a cross-layer system of three layers. One layer uses mobile nodes information such as location and data packets on the network layer in MAC layer protocol as well as full-duplex interfaces in PHY layer. The main concentration of this work is to enhance the security against the Black Hole attacks in the Cross-Layer environment [6] [7].

In war zones, there is no possibility of having an administrator arranged model. A MANET based network can be adequately sent in such zones and help in fitting coordination among the different peers. A specially designed Ad-hoc system can be utilized a mid-movement for family unit applications, in telemedicine, for the virtual route, and so on. These services are to be monitored at some level. Wireless systems administration is a rising innovation which grants users to get to data and administrations, without considering about their information like position, structure, and packet information at MAC and PHY layer.

A focal test in the outline of MANET systems is the advancement of effective MAC and mobile ad-hoc protocols that can proficiently discover courses between the conveying nodes. With an end goal to enhance the execution of cross layer designed system, there has been expanded enthusiasm for protocol that depend on associations between various layers. Cross-Layer Design has turned into the new pattern in cross layer communication systems it tries to improves the limit of wireless communication system through the joint enhancement of various layers in the system [8]-[12].

Cross-layer configuration underscores on the system execution enhanced by enabling distinctive layers of the communication stack to share state data or to facilitate their activities keeping in mind the end goal to together advance system performance. It is a human mindset and brain research that if another plan worldview is proposed, we contrast it and the current one. Henceforth the idea of cross-layer configuration must be contrasted and the conventional layered engineering with the goal that individuals can be motivated towards the utilization of the layered plan.

The cross-layer approach can be alluded to as a network protocol configuration in view of currently using the reliance between protocol layers to improvement of the system performance. This contrasts from the conventional layered approach where the conventions at the distinctive layers are composed freely.

The outline of the paper is given below: section 2 discuss about the methodology adopted carrying out the work. Simulation setup with simulation parameters and the result obtained are shown in section 3. Finally, the paper is concluded in section 4.

2. METHODOLOGY

The objective of paper is to utilize Cross Layer for MAC and PHY Layer data at the directing to enhance the worldwide performance of the system. By utilizing cross-layer association amongst MAC and routing layer with the assistance of network performance QOS parameter like control packet, successful

deliver of packet at destination, energy consumption, network throughput as well as most important average delay during the network execution based on the network simulation time or increased network density, it performs much superior to anything utilizing routing protocol and MAC layer independently. The objective of executing a cross-layer procedure for routing system is to discover the great way that is dependable and effective.

There are attacks like DOS, Sybil and Black Hole attack. Here, Black Hole attack is used in the Cross-layer network, it's a malicious node that promote a best and shortest path for all the source towards the network destination. At a stage where route is set up, then error node forwards it. Moreover, forwarding the data packets from the source node to malicious attacks, the packets were dropped thereafter [13] [14].

Nodes drop out to appreciate the system performance or when setup node drops out then network performance reduced. All system transfers occupied packet to an exact position node that does not exist at all in the network. There are two opportunities for Black Hole attack in MANET. Communication between one mobile nodes to another mobile node declines the communication. At that point, the new mobile node tries to communicate with next, however, the position stills be the same. When the communication begins with other mobile node and all of a sudden dropout the communication interface with the neighbor node then magnification will occur. Since this mobile node are out of the routing task, numerous mobile nodes were associated. When the attacker node gets a RREQ data packet information, it generates a false RREP data packet information. With receiver pre-arrangement, other sender of data packet generates the node expectations that the Black Hole mobile nodes are interconnected with attacker node in place of the receiver [15] [16].

In this scenario, Black Hole attacks are represented which acts as a malicious node within the network topology shows in Fig.1.

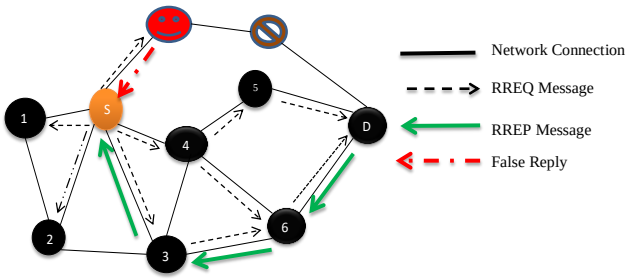

Fig.1. Black Hole attack topology

The Malicious attacker in MANET are categories into two primary classifications: active and passive attackers [17]. In case of a passive attacker, the malicious node characterizes an unapproved control of some association and get data access without infusing false alarm by proving himself as a legitimate node. In case of active attacker, the attacker disturbs the typical working of the system, it can insert drop, or alter packet information [16]. In this case there is a real violation either on arrangement of the network resources or the transmitted information which interrupt the routing protocol procedure, the fatigue of system resources such as equipment failure and communication break during the simulation.

The Black Hole attack is notable system attacker or it could be an attacker on the network [17]. It is classified as an active attack. This Black Hole attack presents a genuine issue for the security purpose, in which the Black Hole attacker inserts the false data information that behave as the final destination node. It sends back-to-back routing packets and data packet to all other node that are having the best path to reach the destination node [16]. When the attacker node gets a RREQ data packet information, it generates a false RREP data packet information in which the sequence number field in the routing Table.is set to a higher value with the lower number of hopes [17]. If the Black Hole attacker has dominant to pick up the way, it can capture every single transmitted data packet before the drop of these packets or loss of information [17].

3. SIMULATION AND RESULTS

Result analysis is the main part for any network and/or system. The simulation of the technique with the simulation parameter tabulated in Table.1 is done using the NS-3 simulator. NS-3 supports the code written in C++/Python for simulation purpose. The performance of the proposed technique is evaluated using QoS parameter like network delay, network throughput, packet delivery ratio and average energy consumption.

The performance of cross layer, Black Hole-cross-layer and detection schema of Black Hole attack in cross-layer with the help of NS-3 (NS-3.17), the scenario consists of 200 numbers of mobiles nodes with the malicious node. The movement of mobile node based on the random way point mobility model [5].

Table.1. Simulation parameter

Parameters	Values
Operating System	(Ubuntu 14.04)
NS-3 version	NS-3.17
Node Variation	50, 100, 150, 200
Packet Size	512
Traffic Type	CBR
Simulation Time	10, 20, 30, 40, 50 Second
Antenna Type	Omnidirectional
Transmission Range	1000×1000 m
Routing Protocol	AODV
Attacker	Black Hole
Detector	AD-Detector

For the analysis of performance of network using considered routing protocols of the MANET systems- AODV Protocol with Black Hole attack developed and designed for Cross Layer Optimization. Here shows the comparison of QOS parameter of the current study based on the mentioned parameter [9].

3.1 PERFORMANCE METRICS

3.1.1 Network Delay:

Average Network delay expressed the simulation time which data packets information send from source to destination nodes though since delays originated by propagation, buffering and queuing and delays. Mathematically formulation of the average delay (*D*) in the network scenario shown in Eq.(1).

Average delay (D) =

$$\frac{\sum_{i=1}^{n}\left(\begin{pmatrix}\text{Received Packet}\\ \text{Time}\end{pmatrix}-\begin{pmatrix}\text{Sent Packet}\\ \text{Time}\end{pmatrix}\right)*1000ms}{\text{Total number of packets delivered}\,(n)} \quad (1)$$

3.1.2 Network throughput:

The mathematical formulation of network throughput shown in Eq.(2), network throughput is the ratio of Packet Size of i^{th} data packet reached to destination end and difference the Packet Arrival and Packet Start time.

$$Throughput = Packet\ Size/(PacketArrival\text{-}PacketStart) \quad (2)$$

3.1.3 Packet Delivery Ratio (PDR):

PDR are measured the ratio of total received data information packets towards destination and total sends data packet from the source nodes. The mathematically formulation of PDR shown in Eq.(3)

$$PDR=\frac{\sum Total\ packets\ received\ by\ all\ destination\ nodes}{\sum Total\ packets\ send\ by\ all\ source\ nodes} \quad (3)$$

3.1.4 Average Energy Consumption:

The network energy consumption is the summation of total spend energy of all nodes in the network.

3.2 RESULTS AND ANALYSIS

Here we define three different scenarios based on the network density and rapidly change network are simulated. Here, the results are represented in three different scenarios presented that are presented in Table.2-Table.7.

Table.2. Delay Comparative Table for AODV-CL, BH-AODV-CL and AD-AODV-CL using (a) Network density

No. of Nodes	AODV-CL	BH-AODV-CL	AD-AODV-CL
50	0.173348	0.333751	0.173348
100	0.179452	0.153694	0.179452
150	0.190753	0.118322	0.190753
200	0.20993	0.154343	0.20993

(b) Simulation time

Simulation Time	AODV-CL	BH-AODV-CL	AD-AODV-CL
10	0.173348	0.154343	0.173348
20	0.212424	0.24549	0.212424
30	0.14199	0.280682	0.14199
40	0.20993	0.820268	0.20993
50	0.15399	0.958874	0.15399

Table.3. PDR Comparative Table for AODV-CL, BH-AODV-CL and AD-AODV-CL using (a) Network density

Nodes	AODV-CL	BH-AODV-CL	AD-AODV-CL
50	97	49	97
100	97	21	97
150	97	10	97
200	97	8	97

(b) Simulation time

Simulation Time	AODV-CL	BH-AODV-CL	AD-AODV-CL
10	97	4	97
20	100	4	100
30	98	2	98
40	99	3	99
50	98	4	98

Table.4. Throughput Comparative Table for AODV-CL, BH-AODV-CL and AD-AODV-CL using (a) Network density

No. of Nodes	AODV-CL	BH-AODV-CL	AD-AODV-CL
50	175837	24421	175837
100	167449	23412	167449
150	139300	32178	139300
200	151103	35306	151103

(b) Simulation time

Simulation Time	AODV-CL	BH-AODV-CL	AD-AODV-CL
10	175837	901042	175837
20	162880	131833	162880
30	433228	50178	433228
40	767747	35455	767747
50	1002263	14366	1002263

Table.5. Energy Comparative Table for AODV-CL, BH-AODV-CL and AD-AODV-CL (a) Network density

No. of Nodes	AODV-CL	BH-AODV-CL	AD-AODV-CL
50	0.871	1.54783	0.89948
100	0.992	1.29354	0.95424
150	1.012	1.90326	1.10979
200	1.159	1.94668	1.39394

(b) Simulation time

Simulation Time	AODV-CL	BH-AODV-CL	AD-AODV-CL
10	0.7748	1.154343	0.8848
20	0.8424	1.549	0.9424
30	0.9919	1.280682	1.09919
40	0.9939	1.868	1.09939
50	1.15399	1.958	1.599

Table.6. Packet Loss for AODV-CL, BH-AODV-CL and AD-AODV-CL using (a) Network density

No. of Nodes	AODV-CL	BH-AODV-CL	AD-AODV-CL
50	2	50	2
100	2	78	2
150	2	89	2
200	2	91	2

(b) Simulation time

Simulation Time	AODV-CL	BH-AODV-CL	AD-AODV-CL
10	2	91	2
20	0	95	0
30	2	95	2
40	0	96	0
50	0	94	0

Table.7. Redundancy Gain for AODV-CL, BH-AODV-CL and AD-AODV-CL using the following (a) Network density

No. of Nodes	AODV-CL	BH-AODV-CL	AD-AODV-CL
50	97	49	97
100	97	21	97
150	97	10	97
200	97	8	97

(b) Simulation time

Simulation Time	AODV-CL	BH-AODV-CL	AD-AODV-CL
10	97	8	97
20	100	4	98
30	98	4	98
40	99	3	99
50	97	5	97

The average delay of AODV-CL is increased with a number of nodes but after 100-node, the delay is increased smoothly. The overall performance of average delay for AODV-CL Black Hole attack with respect to a number of nodes variation or simulation time is higher as compared to the AODV-CL. The Packet Delivery Ratio (PDR) of Black Hole-AODV-CL is constant at 100% for all the network density considered in the network scenario.

With the variation of network simulation time for the AODV-CL system, the PDR shows some variations. However, Black Hole AODV-CL with respect to simulation time, AODV-CL is performing better than the BH-AODV-CL.

The performance of the network throughput for Black Hole-AODV-CL and Black Hole-AODV-CL are almost same for 50, 100,150 and 200 nodes. Moreover, based on the simulation time, the network throughput shows much variation after 20 sec of network running time. Further, BH-AODV-CL shows very low throughput performance as compare to other two scenario under consideration.

The energy consumption of Black Hole in AODV-CL network is continuously increasing as compared to the AODV-CL, which is due to the higher computation time.

4. CONCLUSIONS

In this paper a cross layer design based on the power control, link production in the MANET is proposed for the detection of Black Hole attack. The proposed design was implemented in NS-3 and the obtained results were analyzed for the cross-layer network using MAC and PHY layer, further modifications in the existing schemes of the MANET network is done.

Here, three different scenarios based on network density and rapidly changing topology stages were taken into account. The three different scenarios are firstly the cross-layer network using AODV routing protocol with the presence of any malicious node in the network. Secondly, cross layer network using AODV routing with the presence of Black Hole attack in the network. Thirdly, AD-Detection to detect the Black Hole attack in the cross-layer network.

The network attacker reduced the performance of the cross-layer network with AODV routing by dropping the data packet information during the source to destination communication, while maintaining the throughput and packet delivery ratio of the network. We used cross layer-based detection method to detect the Black Hole attack and improved the network performance. Our result showed that BH-AODV-CL perform lower as delay is more. AODV-CL and AD-AODV-CL perform almost equally in case of PDR and throughput and AODV-CL consumes the minimum energy and hence perform better than the remaining two techniques.

REFERENCES

[1] M. Arifuzzaman, M. Matsumoto and T. Sato, "An Intelligent Hybrid MAC with Traffic-Differentiation-based QoS for Wireless Sensor Networks," *IEEE Sensors Journal*, Vol. 13, No. 6, pp. 2391-2399, 2013.

[2] S. Ping, A. Aijaz, O. Holland and A.H. Aghvami, "SACRP: A Spectrum Aggregation-based Cooperative Routing Protocol for Cognitive Radio Ad-Hoc Networks," *IEEE Transactions on Communications*, Vol. 63, No. 6, pp. 2015-2030, 2015.

[3] J. Wang, D. Li, G. Xing and H. Du, "Cross-Layer Sleep Scheduling Design in Service-Oriented Wireless Sensor Networks", *IEEE Transactions on Mobile Computing*, Vol. 9, No. 11, pp. 1622-1633, 2010.

[4] C.C. Weng, C.W. Chen, P.Y. Chen and K.C. Chang, "Design of An Energy-Efficient Cross-Layer Protocol for Mobile Ad Hoc Networks", *IET Communications*, Vol. 7, No. 3, pp. 217-228, 2013.

[5] L. Karim and N. Nasser, "Reliable Location-Aware Routing Protocol for Mobile Wireless Sensor Network," *IET Communications*, Vol. 6, No. 14, pp. 2149-2158, 2012.

[6] L. Zhang and Y. Zhang, "Energy-Efficient Cross-Layer Protocol of Channel-Aware Geographic-Informed Forwarding in Wireless Sensor Networks," *IEEE Transactions on Vehicular Technology*, Vol. 58, No. 6, pp. 3041-3052, 2009.

[7] X. Ji, Y. He, J. Wang, W. Dong, X. Wu and Y. Liu, "Walking Down the STAIRS: Efficient Collision Resolution for Wireless Sensor Networks", *Proceedings of IEEE International Conference on Computer Communications*, pp. 961-969, 2014.

[8] J. Ben-Othman and B. Yahya, "Energy Efficient and QoS based Routing Protocol for Wireless Sensor Networks", *Journal of Parallel and Distributed Computing*, Vol. 70, No. 8, pp. 849-857, 2010.

[9] Sandeep Sharma and Rajesh Mishra. "A Cross Layer Approach for Intrusion Detection in MANETs", *International Journal of Computer Applications*, Vol. 93, No. 9, pp. 34-41, 2014.

[10] X. Yang and L. Wang, "A Multichannel Transmitting and Assistant Nodes MAC Protocol for Mobile Ad Hoc Networks", *Proceedings of IEEE International Conference on Global Communication*, pp.1-5, 2015.

[11] V. Nguyen, O.T.T. Kim, T.N. Dang and C.S. Hong, "Improving Time Slot Acquisition through RSU's Coordination for TDMA-based MAC Protocol in VANETs", *Proceedings of International Conference on Information Networking*, pp. 406-411, 2016.

[12] S.H.R. Bukhari, M.H. Rehmani and S. Siraj, "A Survey of Channel Bonding for Wireless Networks and Guidelines of Channel Bonding for Futuristic Cognitive Radio Sensor Networks", *IEEE Communications Surveys and Tutorials*, Vol. 18, No. 2, pp. 924-948, 2016.

[13] A. Mohammed, H.S. Boukli and F. Kamel Mohamed, "A Cross Layer for Detection and Ignoring Black Hole Attack in MANET", *International Journal of Computer Network and Information Security*, Vol. 7, No.10, pp. 42-49, 2015.

[14] S. Sharma, R. Mishra and K. Singh, "Current Trends and Future Aspects in Cross-Layer Design for the Wireless Networks", *Proceedings of International Conference on Computer Science and Information Technology*, pp.283-296, 2012.

[15] Sandeep Sharma and Mukul Saini, "Black Hole Attack Detection and Prevention Mechanism for Mobile Ad-Hoc Networks", *Proceedings of IEEE 3rd International Conference on Computing for Sustainable Global Development*, pp. 2993-2996, 2016.

[16] Y.A. Huang, W. Fan, W. Lee and P.S. Yu, "Cross-Feature Analysis for Detecting Ad-Hoc Routing Anomalies", *Proceedings of International Conference on Distributed Computing Systems*, pp. 478-487, 2003.

[17] S. Dhama, Sandeep Sharma, and Mukul Saini, "Black Hole Attack Detection and Prevention Mechanism for Mobile Ad-Hoc Networks", *Proceedings of IEEE 3rd International Conference on Computing for Sustainable Global Development*, pp.2293-2296, 2016.