IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 5, May 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305076 |

Application-Defined Network Using Band Cover Channel in a Deceptive Worm Hole Attack

Harini G [1], Mahalakshmi B [2], Subhashini S [3], Suvathi N [4], Mr. N.Kumaresan [5]

BE Scholars, Department of Computer Science and Engineering, Vidyaa Vikas College of Engineering and Technology, Tiruchengode, Tamilnadu, India[1234]

Associate Professor, Department of Computer Science and Engineering, Vidyaa Vikas College of Engineering and Technology, Tiruchengode, Tamilnadu, India[5]

ABSTRACT: Link Layer Discovery Protocol (LLDP), which is widely used by the controller in Software-Defined Networking to discover the network topology, has been demonstrated to be unable to guarantee the integrity of its messages. Attackers could exploit this vulnerability to fabricate LLDP packets to declare a false link connecting two distant switches to the controller. By doing so, the controller would be misled to route flows to the false links, which leads to further DoS, eavesdropping and even hijacking attacks. This attack seems very similar to the well-known Worm-Hole Attack in wireless sensor networking (WSN).Nevertheless, in WSN, attackers are assumed to leverage an out of-band wired channel to achieve the true packet transmission between the two cheating sensor nodes. We propose two efficient methods for separating the valid RSSI observations of behaving nodes from those falsified by malicious participants. Further, we note that prior signal print methods are easily defeated by mobile attackers and develop an appropriate challenge-response defense.

KEYWORDS: Wormhole attack, WSN, Security, Malicious node

I. INTRODUCTION

The emergence of Software-Defined Networking (SDN) has provided a new network design for future networks. Different from the legacy network, SDN separates the control plane from the data plane, which provides a holistic network topological visibility and flexible programmability. Many enterprises show a great interest in it, and some, for example, Google data centers, have already deployed such technology in their network.

In a normal SDN network, with the help of Open Flow Discovery Protocol (OFDP) referring to Link Layer Discovery Protocol (LLDP), the controller could discover the network topology. However, there are two main vulnerabilities in LLDP: (1) The simple semantics of LLDP makes it easy to falsify the LLDP packets; (2) There is no authentication to ensure the integrity of LLDP packets. Because of these weaknesses, the Link Discovery Service of SDN has been demonstrated as unsecure. The study of topology poisoning in SDN is still in the infancy stage [4]. Hong et al. [3] exploit these vulnerabilities to fabricate LLDP packets to declare a bogus link connecting two distant switches which are not linked in fact. As a result, the SDN controller would acquire a wrong network topology, and forward the data flows to the fabricated link. This would cause further DoS, eavesdropping and even hijacking attacks, which are extremely serious attacks.

Nevertheless, this attack is prone to be detected by the controller as the packets cannot be really transmitted over the forged link. It would produce 100% packet loss when flows are misguided to this link. A simple way to address this problem is by building an out-of-band wired channel between the two switches. However, considering these two switches could be extremely distant, this idea is obviously too expensive. In fact, this attack seems quite similar to the well-known Worm-Hole Attack in wireless sensor networking (WSN).

In their scenario, two compromised sensor nodes, which are out of radio transmission range, falsely declare to others that they are within the transmission range so as to attract packets to go through them that should never go in the first place. Moreover, the two cheating nodes are assumed to be connected by an out-of-band wired channel, and thus, the packets can be then forwarded from one compromised node to another and few packet loss occur. This assumption is reasonable because the network environment in WSN could be much more complex and diverse than that in SDN, and it is entirely possible for some nodes having been connected to existing wired network besides the wireless network. In

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305076 |

contrary, most switches in SDN usually belong to one wired network and have no such out-of-band links, which makes launching this worm-hole attack in SDN much more challenging than in WSN.

II. LITERATURE SURVEY

Several algorithms and scientific studies that have been devoted for MANET. Some of these algorithm require specialized hardware or incur high communication overhead. However, we will concentrate on literature on some of the prevailing solutions on MANET and give brief description of all the relevant literature reviewed.

Chiu and Lui [1] propose wormhole detection method called delay per hop indication (DELPHI). DELPHI perform multipath approach and calculates mean delay per hop of every path. The sender calculate mean delay per hop of each route. Thus, wormhole nodes can be detected if the path that has longer delays and will not be selected to transmit the data packet. Due to the information and detection that DELPHI perform at the sender, it does not require synchronized clock to determine the positioning of the node.

Amish and Vaghela [2] proposed an extension to AODV to detect wormhole attack called Ad-hoc On-demand Multipath Distance Vector routing protocol (AOMDV). the proposed method based on RTT calculation from the source to destination for every route, then, it divide the value of RTT by corresponding hop count and the average value is a threshold value and compare the RTT value with the threshold to determine the existence of wormhole.

Tun and Maw [3] proposed a wormhole detection mechanism based on RTT and neighbour number. The consideration in here is that the adversary can increases the number of neighbours of the nodes within the radius, to provide inaccurate RTT value between successive nodes. Therefore, when the RTT value between two successive nodes is high and the neighbour number is considerable greater than the average neighbour number, there is a suspect that a wormhole path is in between.

Capkun et al. [4] proposed a method called secure tracking of node encounters (SECTOR) against wormhole attack. The distance between two nodes can be calculated based on the speed of data transmitted. The detection method measure the time between sending out a challenges bit and receiving the response, the first node will compute an upper bound of the distance which is between these two nodes, after than, check whether this distance violates and physical constraints.

Lai [5] proposed a method against wormhole attack, by applying the standard routing protocol IPv6 for Low Power and Lossy Networks (RPL). However, this approach delimits the maximum distance that a packet can take in the transmission. The rank of a node defined RPL is adopted to measure the distance. The proposed detection method discovers malicious wormhole nodes if unreasonable rank values are identified.

Hu et al. [6] proposed wormhole attack detection mechanism based on packet leashes. The proposed methodology consider both geographical and temporal leashes. The geographical rely on current location and transmission time associate with the packet. The receiving node will compute the distance to the sender and the time it took the packet to traverse the path to determine whether the packets recipient within a certain distance from the sender. In temporal leashes, based on clock that is tightly synchronized but do not rely on GPS information. The sending node will associate the transmission time and the expiration time to every sent packet to restrict the packet to travel over long distances, and at the receiving node will use its own packet reception time for verification. By using compute lightweight operations which will determine whether the packet pass through the wormhole path.

Hu and Evans [7] proposed mechanism based on directional antennas to prevent wormhole attacks. Neighbour lists will be built in a secure way by using the direction in which a signal is heard from a neighbour with the assumption that the antennas on all the nodes are aligned. However, it only prevents the kind of wormhole attacks in which malicious nodes try to deceive two nodes into believing that they are neighbours.

Chen et al. [8], proposed a distance-consistency-based secure localization scheme that is employed against wormhole attack. It consist of three different phases of detection of wormhole attack. Firstly, detect and identifies whether it is under a duplex wormhole attack or a simplex wormhole attack. And second, the valid locator's identification, different identification schemes are proposed to identity the V-locators. Third, self-localization, after identifying the V-locators, the sensor conducts the self-localization using the MLE method with correct distance measurements.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305076 |

Jamali and Fotohi [9] proposed a method against wormhole attack through Artificial Immune System (AIS) which is able to protect against a set of extraneous attacks without affecting the overall performance of the network. The proposed approach consist of two phases, in the first phase a test packet will be employed and sent from each route and the destination is obliged, a confirmation packet will be send upon receiving test packet. Thus, if the route contain wormhole nodes, the packet will not reach its destination and validation packet will not be received. While in the second phase, usually wormhole attack having lower hop count compare with actual nodes. Thus, when having a low number of hop counts in a route, the possibility of pollution of this route would increase. Which is the situation with a low round trip time and an increase of total energy of the existing nodes in the route.

Tamilarasi and Santhi [10] proposed a method against wormhole attack in MANET through identifying the wormhole and select the best path. Initially, several path will be generated between source and destination called 'K' using Ad-hoc on demand Multipath Distance Vector (AOMDV) routing protocol. Then, the wormhole attacked path will be identifies through source node by verifying the Detection Packet (DP) and Feedback Packet (FP) from the destination. After determine the wormhole attacked paths, the source node will selects the best path among the attacker free paths using Particle Swarm Optimization (PSO) algorithm and forwards the data to the destination through the best path.

III. SYSTEM ANALYSIS

EXISTING SYSTEM

Exploit these vulnerabilities to fabricate LLDP packets to declare a bogus link connecting two distant switches which are not linked in fact. Attacker nodes are detected by analyzing the signal strength of malicious node and also by analyzing distance estimation, the nodes are detected.

DRAWBACKS

- Flows misguided to the fake link will cause 100% packet loss
- More communication overhead.
- It assumes that all nodes, including attackers, remain stationary.
- Consume more energy.
- Less flexible
- Security is the main problem

PROPOSED SYSTEM

The first True worm-hole attack in SDN, which could achieve packet transmission over the forged link without using any out-of-band channels. Received Signal Strength based position verification is more promising as compared to other worm hole attack detection techniques because it is lightweight and does not require centralization. Nodes can locally determine their locations through received signal strength variations and inform neighbors about location updates accordingly. In position verification, network nodes verify the position of each node and further ensure that each physical location is bounded by only one identity at any particular time. To detect moving attackers, note that successive transmissions from the same stationary node should have the same signal print, while attackers cannot quickly (i.e., in milliseconds) switch between precise positions and therefore have inconsistent signal prints . They did not further develop or evaluate a method making use of this observation. We prove conditions under which a participant can fully separate true and false observations.

ADVANTAGES

- Signal print is used to detect the attacker node.
- Communication overhead reduced.
- Easily identify the moving attacker node, it detects and reject the moving nodes.
- Less energy
- More flexible
- Secure communication establishment

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305076 |

IV.METHODOLOGY

IMPLEMENTATION TOOL

NS2 (Network simulator 2)

NS2 is an open-source event-driven simulator designed specifically for research in computer communication networks. NS2 has continuously gained tremendous interest from industry, academia, and government. Having been under constant investigation and enhancement for years, NS2 now contains modules for numerous network components such as routing, transport layer protocol, application, etc. NS Version 2 included a scripting language called Object-oriented Tool cl (OTcl). It is an open source software package available for both Windows 32 and Linux platforms. NS-2 has many uses including:

- To evaluate the performance of existing network protocols.
- To evaluate new network protocols before use.
- To run large scale experiments not possible in real experiments.
- To simulate a variety of IP networks

Proposed Methodology

The main objective for designing the system is to apply Neighbor list based detection algorithm along with Collision avoidance algorithm for the security of mobile ad hoc networks. It also improves throughput and decrease routing delay by using DSDV routing protocol. It maintains a routing table, which lists all available destinations, the metric and next hop to each destination and a sequence number generated by the destination node. Using such routing table stored in each mobile node, the packets are transmitted between the nodes of an ad hoc network. Each node of the ad hoc network updates the routing table with advertisement periodically or when significant new information is available to maintain the consistency of the routing table with the dynamically changing topology of the ad hoc network. The routing table gives the path distance to each destination and best route to get there. To maintain the table up to date, each router exchanges information with all its neighbors periodically. The minimum distance to any neighbor of a node changes, then the process will be repeated until all the nodes have updated the routing information.

ARCHITECTURE

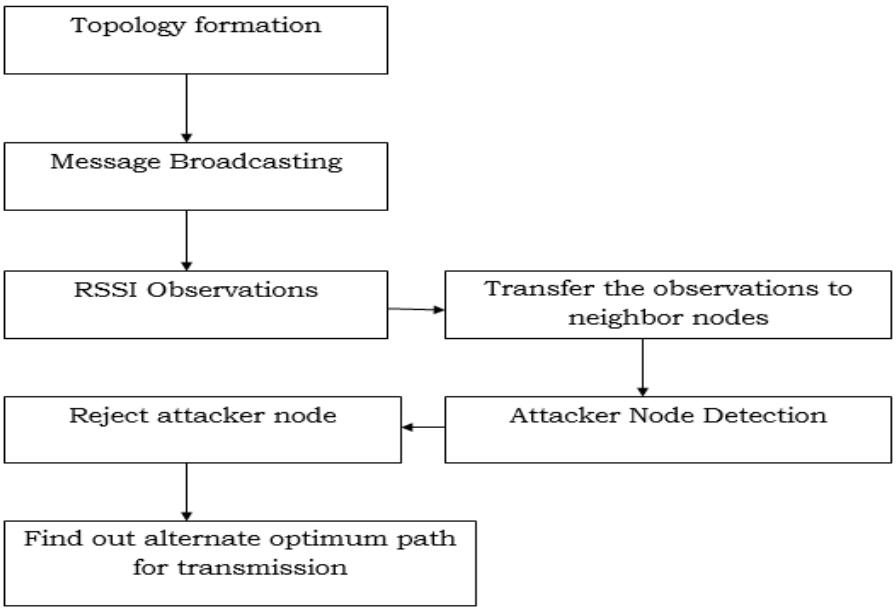

Fig.1 System Architecture

- **Topology formation**
- **Message broadcasting**
- **RSSI observations**
- **Attacker node detection**

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305076 |

Topology formation
Constructing Project design in NS2 should takes place. Each node should send hello packets to its neighbor node which are in its communication range to update their topology.

Message broadcasting
In this module the source node send the packets to the destination. Each and every nodes broadcast their packets to their neighbor node.

RSSI observations
It separates the valid RSSI observations of behaving nodes from those falsified by malicious participants. Received Signal Strength indication is a location based algorithm. It uses the location to detect the attacker node.

Attacker node detection
It includes signal print to detect the attacker nodes in the Wireless Sensor Network. Each node monitors the neighbor nodes which are in their coverage. If it detects any malfunction in the network, it reports to the base station.

V.RESULT

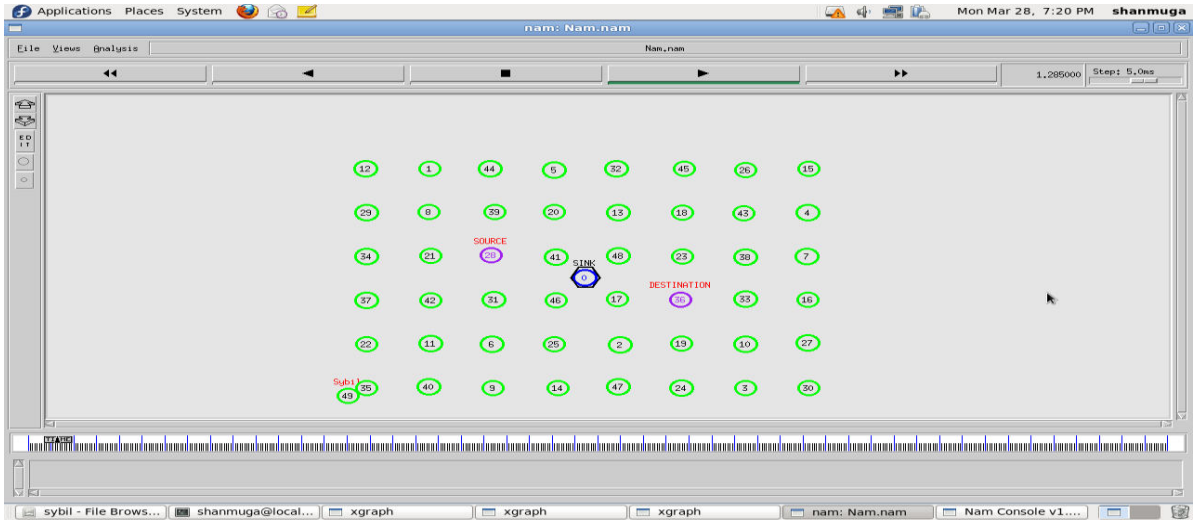

Fig 5.1: Node creation and Topology formation

In the above output screen display the no.of.nodes created and topology formation in NAM window shown in Fig 5.1.

Fig 5.2: RSSI Informs attacker to the sink node

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305076 |

In the above figure detects the attacker node and schedules the awake up region. Then RSSI informs attacker node to the sink as shown in Fig 5.2.

Fig 5.3: Node 47 detects the attacker node 49 and schedules awaken region

In the above figure node 47 detects the attacker node 49 and schedules the awake up region as shown in Fig 5.3.

Fig5.4 Node 48 scheduled to awakened to send the sensed data to the base station

In the above figure schedules the awake up region and sends the sensed data to the base station as shown in Fig 5.4

VI. CONCLUSION

In this paper, we present the Worm-Hole Attack in SDN, which seriously influences the security of data in SDN network. Compared with previous work, our attack realizes communication through the fake link with in-band channels. We have presented a new mechanism of detecting node misbehavior. We have presented reputation and trust based mechanism in detecting attacker in the network. This research described a method to use signal prints to attacker node in open ad hoc and delay-tolerant networks without requiring trust in any other node or authority. We use the inherent difficulty of predicting RSSIs to separate true and false RSSI observations reported by one-hop neighbors. Attackers using motion to defeat the signal print technique are detected by requiring low latency retransmissions from the same position.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305076 |

VII. FUTURE SCOPE

In future works, we intend to enhance the simulation environment so that we can consider a more dynamic attack model. In this phase, we enhance tracking Method to detect Multiple attacker nodes. Since we have to detect multiple attacker nodes, we use only one Sensor node to sense the attacker to reduce the redundancy of the sensed data. In case of failure in any node, the possible node to detect the attacker in the same face will sense the misbehaving nodes. By using this concept we'll reduce the Data Redundancy and Energy Consumption of the network.

REFERENCES

[1] S. Majumder and D. Bhattacharyya, ''Mitigating wormhole attack in MANET using absolute deviation statistical approach,'' in Proc. IEEE 8th Annu. Comput. Commun. Workshop Conf. (CCWC), Las Vegas, NV, USA, Jan. 2018, pp. 317–320.
[2] J. Seo and G. Lee, ''An effective wormhole attack defence method for a smart meter mesh network in an intelligent power grid,'' Int. J. Adv. Robot. Syst., vol. 9, p. 49, Dec. 2012.
[3] S. Amutha and K. Balasubramanian, ''Secured energy optimized ad hoc on-demand distance vector routing protocol,'' Comput. Electr. Eng., vol. 72, pp. 766–773, Nov. 2018.
[4] S. Rezaei, M. Gharib, and A. Movaghar, ''Throughput analysis of IEEE 802.11 multi-hop wireless networks with routing consideration: A general framework,'' IEEE Trans. Commun., vol. 66, no. 11, pp. 5430–5443, Nov. 2018, doi: 10.1109/TCOMM.2018.2848905.
[5] M. Zaminkar and R. Fotohi, ''SoS-RPL: Securing Internet of Things against sinkhole attack using RPL protocol-based node rating and ranking mechanism,'' Wireless Pers. Commun., vol. 114, no. 2, pp. 1287–1312, Sep. 2020.
[6] A. Amara korba, M. Nafaa, and S. Ghanemi, ''Analysis of security attacks in AODV,'' in Proc. Int. Conf. Multimedia Comput. Syst. (ICMCS), Marrakech, Morocco, 2014, pp. 752–756, doi: 10.1109/ICMCS. 2014.6911193.
[7] R. Singh, J. Singh, and R. Singh, ''WRHT: A hybrid technique for detection of wormhole attack in wireless sensor networks,'' Mobile Inf. Syst., vol. 2016, Jan. 2016, Art. no. 8354930.
[8] S. R. M. Jamali; Fotohi; Analoui, ''An artificial immune system based method for defense against wormhole attack in mobile ad hoc networks,'' Tabriz J. Electr. Eng., vol. 47, 4, 2018, pp. 1407–1419.
[9] J. Li, D. Wang, and Y. Wang, ''Security DV-hop localisation algorithm against wormhole attack in wireless sensor network,'' IET Wireless Sensor Syst., vol. 8, no. 2, pp. 68–75, Apr. 2018, doi: 10.1049/iet-wss.2017.0075.
[10] Z. Shi, R. Sun, R. Lu, J. Qiao, J. Chen, and X. Shen, ''A wormhole attack resistant neighbor discovery scheme with RDMA protocol for 60 GHz directional network,'' IEEE Trans. Emerg. Topics Comput., vol. 1, no. 2, pp. 341–352, Dec. 2013, doi: 10.1109/TETC.2013.2273220.
[11] S. Qazi, R. Raad, Y. Mu, and W. Susilo, ''Multirate DelPHI to secure multirate ad hoc networks against wormhole attacks,'' J. Inf. Secur. Appl., vol. 39, pp. 31–40, Apr. 2018.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details