International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-5, January 2020

Misdirection Attack Detection in Wireless Sensor Network

Moirangthem Marjit Singh, Spandan Kumar Barthakur, Thounaojam Rupachandra Singh, Utpal Nandi

Abstract: ***Wireless Sensor Network (WSN) is susceptible to various kinds of security attacks such as the misdirection attack. Detection of misdirection attack in WSN is a difficult job. The malicious node misdirects the arriving packets to a node other than the purposive node in the path from the source to the destination. Consequently, it introduces high end- to- end delay in the network. A novel technique for detection of misdirection attack in WSN without using cluster heads is proposed in the paper. The proposed detection technique has been implemented using Omnetpp 5.4.1 on four different network scenarios (10, 20, 30, and 40 numbers of nodes) and varying number of malicious nodes. The results of simulation shows that the proposed technique delivers better detection rate with reduced end- to- end delay compared to the detection method which uses cluster heads.***

Keywords: Misdirection Attack, Malicious Nodes, Security Wireless Sensor Network.

I. INTRODUCTION

Wireless Sensor Network (WSN) consists of many sensor nodes which is scattered randomly in an area of interest [1][2]. The components of a WSN include sensor node, base station, gateway, patch network and transit network. The sensor nodes are able to sense and process data from the environment. The sensor node is a low cost and has low battery lifetime. The base station collects the sensed data, analyzes it and forwards it to the remote server. The gateway acts as an interface between WSN and other networks. The possibility of quick and easy deployment of WSN makes it very popular for application in various areas namely military, medical science, remote sensing, disaster management etc. Despite its gaining popularity, the WSN is also vulnerable to a number of security attacks [3]. Misdirection attack is a type of Denial of Service (DoS) attack where the data packets are transferred to another node instead of forwarding to an intended node that will ultimately require higher delay and hence decreases network throughput. Misdirection attack is basically of two types: the one where the packets are transmitted to a node nearer to the intended destination node and the other one is where the packets are transferred to a node that is placed at a far distance from the intended destination [4]. The first type of the misdirection attack is less harmful than the second type of misdirection attack [5]. In the first type, packets arrive at the intended destination node through a different path instead of using the defined path. Consequently the network delay becomes longer delivering minimum network throughput performance. The second type of misdirection attack is more harmful as an infinite path may be formed and the packets never reach the target or destination node. This will result in infinite value in maximum delay and giving network throughput performance to be zero [6].

Efforts have been made over the years to develop techniques, methods and algorithms that can precisely detect various security attacks such as wormhole attack [7], black hole attack, misdirection attack etc. in wireless networks. A few techniques for detecting misdirection attack in WSN is reported in the current literature. The various techniques developed to detect the misdirection attack in wireless networks include cluster based detection methods [8], [9]including its variants such as using enhanced LEACH protocol [10] and recursive application of LEACH clustering techniques [11]. In cluster based detection method, a node having the highest energy is the cluster head. The source node keeps tract of the buffer and the buffer has entry for every packet that are transmitted along with a time stamp value as per sequence number of the packets. Buffer allocation is done by the cluster head. The cluster head has information about all packets. It compares the sequence number of the all the packets with the sequence number of those packets transmitted in the defined path as well as the value of time stamp. The previous node in the path will be deleted if a mismatch in the packet sequence number is found. Also a mismatch in time stamp value will lead to detection of a suspicious path. Hence the selection of a favorable path for data transmission begins. In this way the misdirection attacker is identified and detected by the cluster based technique. Using enhanced LEACH protocol the authors in [10] have proposed a method to detect malicious node in WSN.

Manuscript published on January 30, 2020.
* Correspondence Author
Dr. Moirangthem Marjit Singh*, Department of Computer Science & Engineering, North Eastern Regional Institute of Science & Technology, Nirjuli, India. Email: marjitm@gmail.com
Spandan Kumar Barthakur, Department of Computer Science & Engineering, North Eastern Regional Institute of Science & Technology, Nirjuli, India. Email: spandankumarb@gmail.com
Dr. Thounaojam Rupachandra Singh, Department of Computer Science, Manipur University, Imphal, Manipur, India. Email: rupachandrath@manipuruniv.ac.in
Dr. Utpal Nandi, Department of Computer Science, Vidyasagar University, West Bengal, India. Email: nandi.3utpal@gmail.com

A modified version of cluster head selection approach based on lifetime of battery and distance for detection of malicious nodes has been adopted. LEACH clustering techniques has been recursively applied for detection and prevention of DoS attacks in WSN [11]. Here the LEACH algorithm is used to construct clusters. A node that transmits an excess amount of packets than the permitted amount will be considered as a malicious node. All packets transmitted by this malicious node are blocked and a message is broadcasted to all cluster nodes informing it as an intruder node. Topological delay and throughput analysis in wireless sensor network can be seen in [12]. In this paper, an algorithm to detect the first type of misdirection attack is proposed without using cluster head formation and implemented in Omnetpp 5.4.1 simulation software. Simulation results shows that the proposed algorithm delivers better detection rate with reduced end- to- end delay compared to the detection method which uses cluster heads.

II. PROPOSED ALGORITHM

In the proposed algorithm, a path for data transmission in WSN is defined along with assignment of a fixed unit of time (time slice) for the nodes to transmit the data to its next neighboring node in the defined path. A time parameter called start time of each node is calculated by adding with the packet transmission time of the previous node with the current node in the defined path. The difference in the start time of a node with its previous node in the defined path can be compared to detect the presence of a misdirecting node. If the difference in start time of a node is comparatively higher than its previous node, then it can be reasoned out that the previous node had misdirected the packets to some other nodes not present in the defined path. Due to this longer transmission time has taken than the normal time defined for the network. In this way, the misdirecting node in WSN can be detected. The proposed algorithm to detect misdirection attack in WSN is given below.

Input: A WSN under misdirection attack
Output: Attack detection, End- to-end delay

Step 1: Set up a network with n number of nodes.
Step 2: Enforcing Misdirection Attack:
Step 2.1: Set up an optimal path from source to destination.
Step 2.2: Initialize multiple packets for transferring from source to destination in the predefined path.
Step 2.3: For i = 1 to n
Packet[i] = new cPacket("Data");
Step 2.4: Transfer the packets in the predefined path.
Step 2.5: Route the packets to any other node than the ones present in the defined path.
Step 3: Detection Of Misdirection Attack:
Step 3.1: Assign 't1' units of time for transferring of packets from single node to the other in the defined path.
Step 3.2: So for each node,
Start time = Transmission time of the previous nodes in the path + 't1';
Step 3.3: Calculate the start time of transmission for each of the nodes in the path.
Step 3.3.1: If the difference in start time of the node with the previous node is high,then, previous node is a malicious node;
Else, node is a normal node ;
Step 4: End.

III. IMPLEMENTATION AND RESULT ANALYSIS

The proposed algorithm has been implemented using Omnetpp 5.4.1simulation software on four different network scenarios (10, 20, 30, and 40 numbers of nodes) and varying number of malicious nodes and time slice of 2seconds. The observed misdirection attack detection ability using the proposed algorithm is given in Table I. It can be seen that the presence of misdirection attacker node in the wireless sensor network is correctly detected for all WSN configurations as shown in Table I. However, WSN having 10 nodes was small and introduction of 3 or more malicious nodes was problematic. Similarly, WSN having 20 nodes under 4 numbers of malicious nodes was not simulated. Hence a blank entry is indicated for such cases in Table I.

Table I: Observed misdirection attack detection ability

Number of nodes	Number of misdirecting/malicious nodes			
	1	2	3	4
10	Detects	Detects		
20	Detects	Detects	Detects	
30	Detects	Detects	Detects	Detects
40	Detects	Detects	Detects	Detects

The end-to-end delay in milliseconds (ms) obtained through the results of simulation for various WSN configurations in presence of varying number of misdirection attacker nodes are listed in Table II.

Table II: End-to-end delay simulation result using proposed algorithm

Number of nodes	Number of malicious nodes			
	1	2	3	4
10	7.53ms	8.79ms		
20	11.30ms	12.56ms	13.81ms	
30	15.07ms	16.33ms	17.58ms	18.84ms
40	18.84ms	20.10ms	21.35ms	22.61ms

The graphical plot of the end-to-end delay for various Wireless Sensor Networks in presence of 1, 2, 3 and 4 numbers of malicious/misdirection attacker nodes using proposed technique is shown in Figure 1.

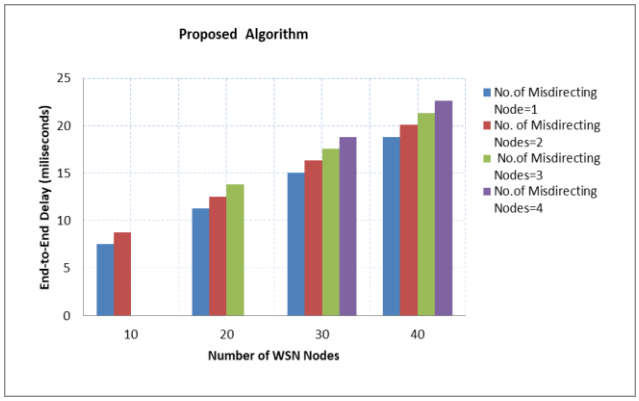

Figure 1: End-to-end delay (Proposed algorithm)

It can be seen from the graphical plot given in figure 1 that the end-to-end delay increases with the increase in number of misdirection attacker nodes in the WSN. Also a gradual increase in the WSN nodes increases the end-to-end delay. This is possible as more routes are available in the network due to increased size of WSN. Figure 2 shows the graphical plot of end-to- end delay parameter for all scenarios of WSN in presence of misdirection attack using cluster based approach. A graphical plot that compares the end-to-end delay parameter of the proposed algorithm and the cluster based algorithm is shown in Figure 3 to Figure 6 for WSN with nodes configuration from 10 to 40 nodes. It is observed from Figure 3 to Figure 6 that the proposed technique performs better than the cluster based technique giving reduced end-to-end delay in all scenarios of WSN.

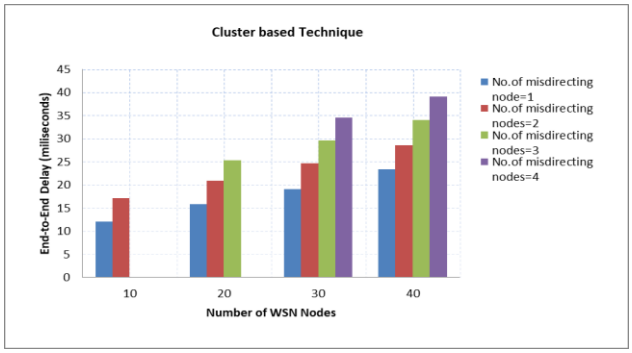

Figure 2: End-to-end delay (cluster based)

The end-to-end delay parameter increases with the increase in the number of misdirecting nodes as shown in Figure 2 using Cluster based approach.

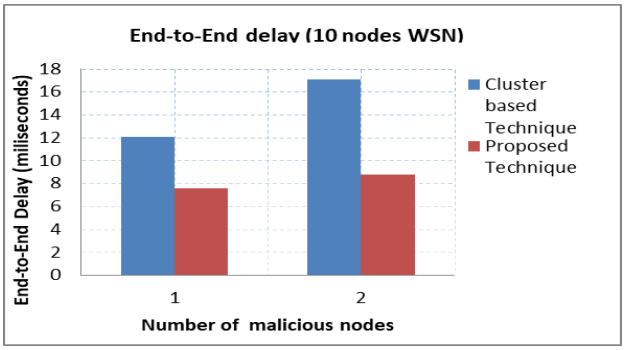

Figure 3: End-to-end delay comparison (10 nodes WSN)

It can be observed from Figure 3 that the end-to-end delay for WSN with 10 nodes using proposed technique is lesser than the Cluster based technique. Hence the proposed algorithm performs better than the Cluster based technique.

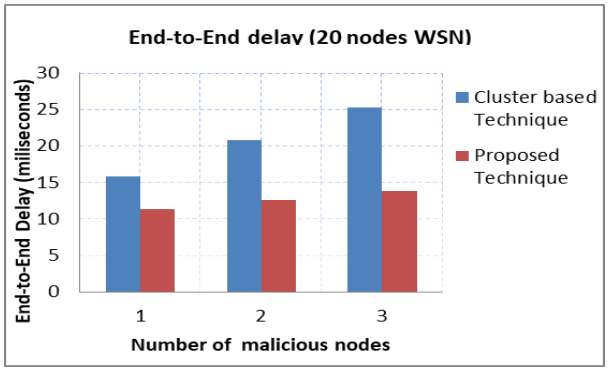

Figure 4: End-to-end delay comparison (20 nodes WSN)

Figure 4 shows that the proposed technique performs better than the Cluster based technique when implemented for WSN having 20 nodes. Similarly, the performance of the proposed algorithm is better than the Cluster based technique for WSN having 20 & 30 nodes as shown in Figure 5 and Figure 6 respectively.

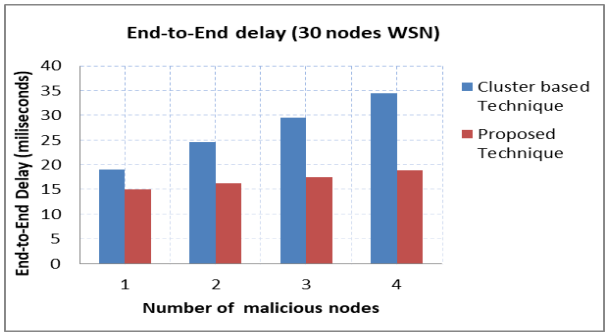

Figure 5: End-to-end delay comparison (30 nodes WSN)

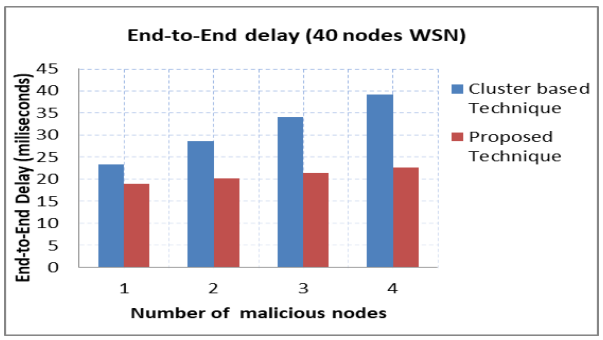

Figure 6: End-to-end delay comparison (40 nodes WSN)

Table III shows the consolidated comparisons of end-to-end delay simulation results (in milliseconds) between cluster based technique and the proposed technique. All Simulations have been carried out using Omnetpp 5.4.1simulation software in windows 7 environment.

Table III: Comparison of end –to-end delay simulation result

No of Nodes	No of Malicious Nodes							
	1		2		3		4	
	Proposed	Cluster based	Proposed	Cluster based	Proposed	Cluster based	Proposed	Cluster based
10	7.53ms	12.05ms	8.79ms	17.05ms				
20	11.30ms	15.82ms	12.56ms	20.82ms	13.81ms	25.23ms		
30	15.07ms	19.05ms	16.33ms	24.59ms	17.58ms	29.59ms	18.84ms	34.55ms
40	18.84ms	23.37ms	20.10ms	28.56ms	21.35ms	34.05ms	22.61ms	39.07ms

IV. CONCLUSION

An algorithm to detect misdirection attack in wireless sensor network has been proposed and implemented in the paper without using cluster heads. It is found from the results of simulation that the proposed algorithm performs comparatively better than the commonly used cluster based algorithms [8][9][10] to detect misdirection attack in WSN by taking lesser end-to end delay parameter. The proposed algorithm may be applied to detect other attacks such as replay attack and routing information protocol attack in WSN.

REFERENCES

1. Sheng Yu, Baoxian Zhang, Cheng Li, and Hussein T. Mouftah.(2014) :Routing Protocols for Wireless Sensor Networks with Mobile Sinks: A Survey, IEEE Communications Magazine,Volume:52, Issue 7,pp 150-157, July 2014.
2. Singh, M.M. and Basumatary, H.(2018),: MERAM-R: Multi-clustered energy efficient routing algorithm with randomly moving sink node,Journal of Scientific & Industrial Research, Vol. 77(01)2018,pp.15-17, ISSN: 0022-4456.
3. Singh, M.M. and Dutta, N.(2017),: Security issues in wireless sensor networks", International Journal of Distributed and Cloud Computing, Vol.5, Issue 2, December 2017, pp.07-16, ISSN: 2321-6840.
4. Saini, M., Kumar,R. and Kaur,J.(2016),: To propose a novel technique for detection and isolation of misdirection attack in wireless sensor network, Indian Journal of Science and Technology, Vol 9(28), July 2016, pp1-7, ISSN: 0974-6846
5. Abdullah,M.Y.,Hua,G.W., Alsharabi,N.(2008): Wireless sensor networks misdirection attacker challenges and solutions(2008)., IEEE 978-1-4244-2184-8/08/
6. Anwar,R.W., Bakhtiari,M., Zainal, A.,Abdullah, A.H., Qureshi,K.N.(2014), "Security issues and attacks in wireless sensor network," World Applied Sciences Journal, vol. 30, no. 10, pp. 1224-1227.
7. Dutta, N. and Singh,M.M.(2019): Wormhole attack in wireless sensor network: A critical review, In: J.K.Mandal et al (eds.), Advanced Computing and Communication Technologies, Advances in Intelligent Systems and Computing 702, pp 147-161. Springer Nature Singapore Pte. Ltd, (2019) DOI: https://doi.org/10.1007/978-981-13-0680-8_14
8. Sachan, R.S., Wazid, M.(2013): A Cluster based intrusion detection and prevention technique for misdirection attack inside WSN, Proceedings of IEEE international conference on communication and signal processing, pp 795-801, April 3-5 2013, India
9. Mansouri, D., Mokdad,L., Ben-othman,J.,Ioualalen,M.(2013): Detecting DoS attacks in WSN based on clustering Technique, Proceedings of 2013 IEEE wireless communications and networking conference(WCNC):NETWORKS, pp.2214-2219.
10. Das, S., Das,A.(2015): An algorithm to detect malicious nodes in wireless sensor network using enhanced LEACH protocol, Proceedings of 2015 IEEE international conference on advances in computer engineering and applications, pp.875-881.
11. Mansouri, D., Mokdad,L., Ben-othman,J.,Ioualalen,M.(2015): Preventing denial of service attacks in wireless sensor networks, Proceedings of IEEE ICC 2015 –mobile and wireless networking symposium, pp.3014-3019.
12. Sachan, R.S., Wazid, M., Singh,D.P.,Katal,A., Goudar, R.H.(2013): Misdirection attack in WSN:topological analysis and an algorithm for delay and throughput prediction. Proceedings of IEEE 7th international conference on intelligent systems and control(ISCO2013), pp.427-432.

AUTHORS PROFILE

Dr. Moirangthem Marjit Singh received his B.Tech and M.Tech degrees in Computer Science and Engineering from North-Eastern Hill University, Shillong, India and North Eastern Regional Institute of Science and Technology, Arunachal Pradesh, India in 2001 and 2010 respectively. He received his PhD (Engg.) degree in Computer Science & Engineering from University of Kalyani, West Bengal, India in 2017. Dr. Marjit has 17+ years of teaching and 10 years of research experience. He has published a number of papers in International Journals and Conference Proceedings. He was awarded the IE(I) Young Engineers Award 2014-2015 in Computer Engineering division by the Institution of Engineers(India) and received the Best Paper Award in ICACCT 2016 International Conference (published by Springer). He was awarded the Gold Medal for getting top position in M.Tech program at NERIST, Arunachal Pradesh, India. Dr. Marjit also secured 1st position in X and 2nd position in XII Examinations conducted by CBSE, New Delhi, India amongst the candidates sent up from Jawahar Navodaya Vidyalayas(JNVs) of eight states of north eastern India in 1995 and 1997 respectively. He is a Fellow of IETE New Delhi, India and Senior Member of IEEE USA. Currently Dr. Marjit is the Head of Department of Computer Science & Engineering at North Eastern Regional Institute of Science & Technology, A Deemed to-be University under MHRD Govt. of India, Arunachal Pradesh India. He is the Joint Secretary of IEI Arunachal Pradesh State Centre, India at present. His research area of interests includes Mobile Adhoc Networks, Wireless Sensor Network, Network Security, AI, Machine Learning and Deep Learning.

Spandan Kumar Barthakur received his B.Tech degree in Computer Science & Engineering from Gandhi Institute of Engineering & Technology, Gunupur, Ordissa, India in 2016. He completed his M.Tech degree in Computer Science & Engineering from North Eastern Regional Institute of Science & Technology, Arunachal Pradesh, India in 2019.

Dr. Thounaojam Rupachandra Singh received his Ph.D in Information Technology from Assam University Silchar, India in 2015 and MCA degree from Manipur University in 2000. He is currently working as Assistant Professor in Department of Computer Science, Manipur University, Imphal, Manipur, India. His research area of interest includes computer network, data structure, watermarking, operating system, Software-Defined Network.

Dr. Utpal Nandi received his M.Tech and Ph.D degrees in Computer Science & Engineering from University of Kalyani, West Bengal, India in 2009 and 2018 respectively. He has 10 years of teaching and research experience. He has published a number of papers in Journals and Conference Proceedings. His research area of interest includes security, image processing, and steganography. He is currently working as an assistant professor in Department of Computer Science in Vidyasagar University, West Bengal, India.