International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6, August, 2019

Mitigation of Selective Forwarding attacks in Wireless Sensor Network

Deepak N. Biradar, T.S. Vishanath

Abstract: ***Security issue in Wireless Sensor Networks (WSNs) is a major problem while dealing with WSNs. Therefore, WSNs are susceptible to various kinds of safety assaults. The restricted capability of sensor nodes is one reason for attacks in sensor networks. In WSNs, on the network layer, there are different kinds of safety attack detection methods. There are also many severe limitations in sensor nodes such as energy efficiency, reliability, scalability that affect WSN safety. As sensor nodes have restricted ability for the majority of the limitations, a selective forwarding attack in the networks is hard to identify. In selective forwarding attack, malicious nodes function as a ordinary nodes. However, it tries to find and crash messages prior to forwarding the packet to further nodes. For keeping this sort of attack aside from networks, we suggest a multi-layer strategy, Selective Forwarding Detection (SFD) that maintains the safe transmission of information among sensor nodes at the same time as detecting the selective forwarding attack. In addition, energy efficiency, reliability and scalability are part of the approach.***

Index Terms: Wireless Sensor Networks, Selective Forwarding Detection,Fuzzy Path Selection.

I. INTRODUCTION

Sensor networks collect information needed to be integrated into smart network environments. These settings include, for instance, transportation, home, army, healthcare, and buildings. WSNs monitoring different physical phenomena are used in military, agriculture, construction or automation, industrial monitoring, etc. Because of the sensor node's limited communication radios, the measurements composed are routed to a Base Station (BS) for dispensation on the basis of hop-by-hop from node to node[1]. In WSN, sensor nodes send packets using wireless communication. Due to their restricted energy and transmission spectrum, sensor nodes produce data packets in Wireless Sensor Networks (WSNs) and forward them towards the Base Station (BS) in a multi hop cooperative way. Packets containing data may get lost due to crash, noise, congestion, or other network problems while being routed to the BS.[17] The supposed packet drop attack refers to a collection of attack wherever compromised nodes deliberately crash packets.[18]WSNs have an impression on the economy and on the industrial sector. It includes countless sensors, these sensors actually interact via radio connections with a large amount of tiny nodes. Sensor networks have a base station and a source. WSN's are running thousands of sensor nodes [2]. Over the past few years, the security issues of wireless sensor networks are widely explored. WSN's are vulnerable to many kinds of attacks as they act as an open network with restricted node resources. Consequently, the primary disadvantage for all devices is the barriers to secure a wireless sensor network. The most common threats to wireless sensor network safety include eavesdropping, compromised node, interrupting, modifying or injecting malicious packets, compromising privacy, and denying service attacks [3]. Due to constraint of both energy and memory, existing security procedures are not appropriate for these wireless sensor networks. However, owing to distributed and open characteristics of the networks and the restricted resource of nodes, they are also extremely vulnerable to attacks. An opponent may compromise a sensor node, modify information reliability, snoop messages, insert false messages, and resource the waste network. DoS (Denial of service) attack is a prevalent attack in WSN, and the attacker's goal in DoS attack is to create target nodes unapproachable to genuine user [4].

II. SELECTIVE FORWARDING ATTACKS

There are many types of attacks on a network layer in WSNs. In addition, by merely refusing to route packets, a sensor node can obtain multi-hop benefits. Thus, with the net result, it could be performed all the time [16]. If a nearby node marks a path through the malicious node, messages won't be modified [5]. Karlof and Wagner first defined the Selective Forwarding Attack[6]. Sometimes this attack is called an attack on the Gray Hole. In a straightforward form of selective forwarding attack, nodes which are malicious try to avoid the packets in the network by denying to send or drop messages transient through them. In a basic manner of selective forwarding attack, malicious nodes attempt to prevent the network packets by denying forwarding or dropping emails that pass across them. Selective forwarding attacks come in distinct types. In one kind of the selective forwarding attack, the malicious node can crash the packets forming a group of nodes or a specific node selectively. For that specific node or node group, this behavior creates a DOS attack. If all the packets are dropped, this attack, only be called as a black hole attack [7]. The Blind Letter attack [8] is another type of selective forwarding attack.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
Deepak N. Biradar*, Computer Science and Engineering, Lingaraj Appa Engineering College, Bidar, India.
Dr. T.S. Vishanath, HoD Electronics and Communication Engineering, BKIT, Bhalki, India.

The concept of this attack is that it should be ensured with arbitrarily malicious nodes that the node to which the forward-hop node is transmitting the packet
which is relaying is in fact a neighbor of the forward-hop node. Neglecting attack is one which acknowledges the source for reception and drops data thereafter. When the priority is only given to its own packets not to others, it is known as greedy attack.

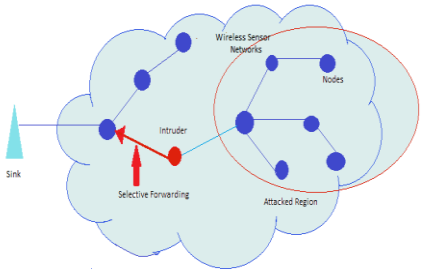

Fig 1: Selective Forwarding Attack

III. LITERATURE SURVEY

In [9], Bin Xiao et al., proposed CHEMAS (CHEckpoint-based multi-hop recognition scheme), a lightweight safety system for selective forwarding attack detection. The suggested system can arbitrarily pick portion of middle nodes along a forwarding route as check point nodes to generate recognition for each received packet. Yuan yuan Zhang et al[10], First, simulated and evaluated the impacts on both information flows and ACK flows of selective forwarding attacks and then explored the multi-path recognition safety capacities. JuRen et al,[11] proposed an adaptive detection threshold (CRS-A) channel-aware reputation scheme to detect selective forwarding attacks in WSNs. The CRS-A evaluates sensor node information transmission behaviors based on the deviation of the controlled packet loss and the estimated ordinary number. To optimize CRS-A's detection precision, we theoretically obtain the ideal forwarding evaluation threshold that is adaptive to the time-variant channel situation and the predictable attack probability of compromised nodes. In addition data forwarding system which is attack-tolerant is being created to work with CRS-A to stimulate the forwarding cooperation of compromised nodes and improve the network's information distribution ratio. Martin Stehlik et al,.[12] Two parameterized collaborative invasion detection techniques were proposed and their parameters were optimized for specific scenario using broad simulations and multi-objective evolutionary algorithms. Meghana Shinde et al.,[13] used The active trust routing system idea to protect multiple types of attacks during data packet routing. Such attacks consist primarily of black hole attack, service denial attack and selective forwarding attack. The scheme also protects information by using the ECC algorithm, which offers safety, to hide the information during routing.Experimental findings showed that the suggested scheme increases safety along with prolonged lifetime of the network and low energy use and increased effectiveness throughout the lifetime of the network.Sert, Seyyit Alper et al.,[14] in their paper, introduced a fuzzy approach that effectively mitigates single selective forwarding attacks in WSNs.The authors simulated and obtain the performance of our suggested strategy and its evaluations. The experimental results demonstrate that the suggested method is an efficient solution for efficiency metrics such as Half of the Nodes Alive (HNA), Packet Drop Ratio (PDR) and Total Remaining Energy (TRE) to serve as a defense mechanism. Devu Manikantan Shila et al.,[15] Developed a channel-conscious detection algorithm (CAD) capable of efficiently identifying selective forwarding misconduct from ordinary channel losses. Two strategies, traffic tracking and channel estimation are based on the CAD algorithm. If the rate of loss monitored at certain hops exceeds the expected normal rate of loss, it will identify those nodes engaged as attackers. The authors also conducted analytical trials to determine the optimum thresholds for identification that minimizes the summing up of missed probabilities and false alarm for identification.

IV PROPOSED WORK

The proposed methodology is divided into two parts:

1. Fuzzy Logic cluster formation

Increasing numbers of clustering-based protocol use fuzzy logic in WSNs for clustering due to the uncertainties in the WSN environments. Uncertainties intrinsic in the WSN nature are addressed efficiently using the blurred input and output variables. And, it has a small complexity in computing and more flexibility than crisp logic. The fuzzy inference system can be used to achieve a better mix of the relevant input parameters in order to achieve optimum performance, which in this context is the CH selection method Using Fuzzy logic, a dynamic CH choice is made. Distances to BS and Residual energy are the Fuzzy input parameters. The output parameter is the likelihood of CH. The crisp inputs were initially mapped into suitable fuzzy sets. The language variables and the following values for the input variables are shown in the table.

Table 1 Parameters and the linguistic variables

Parameters	Linguistic variables
Residual energy	Low, Medium, High
Distance to base station	Close, medium, far
Probability of becoming CH	Very large, large, Rather large, medium large, Medium, Medium small, rather small, medium small, very small

The proposed method uses trapezoidal and triangular membership functions. Triangular membership functions are used for intermediate values and Trapezoidal membership functions are used for border values and t by applying the fuzzification functions, crisp inputs are changed into fuzzy sets and then gathered with if-then rules to get the fuzzy output. The method of defuzzification converts the likelihood of fuzzy output into a crisp value showing a node's likelihood of becoming a cluster head. Once Fuzzy logic determines the likelihood of becoming CH, BS broadcasts its likelihood to all nodes.. The nodes advertise the probability value to its neighbors within the communication range. When no higher probability message is received by a node,
it elects itself as CH.

The CH broadcasts its status to its neighbors. The nodes receiving the CH message, joins the cluster as cluster member. After the formation of clusters, cluster member sense the value and forwards to CH. CH receives the data and aggregates into a single packet. CH forwards the aggregated packet to BS via intermediate CHs.

2. Two phase process is used to mitigate SF attacks.

Here in this work, the authors are considering two phase process for mitigation of Selective Forwarding attacks. That are:

Phase 1: Detection of Malicious node phase

Phase 2: Diffusion of detected nodes from routing table

The proposed protocol uses a forwarding mechanism

Sender Radio Range (SRR) It contains all nodes near to source.

Sender Feasible Candidate (SFC) It is the list of those nodes which are between source and destination and eligible to become next hop candidate.

Phase1: Detection of SF

Detection of malicious nodes is also two phases Suspect node detection:

Step1: Each node sends a message with random non-existent dummy destination messages.

Step2: Grey hole and Black hole nodes sends the rrep that it can transfer the data to destination.

Step3: source node identifies the suspected Black and grey hole nodes.

Step4: Source node sets deadline time to reach to the destination which is called expected latency.

Step5: Source compares the latency of each route leads to the destination by expected latency and takes up next hop decision.

Step6: If latency is more than expected such nodes or routes are identified

Step7: Every node repeats this activity after every periodic interval.

False Positive Phase:

1.Node A and B both are in each other's transmission range. All the nodes are physically identical.

2. All the nodes are considered healthy & runs same process

3. T=1 is equal to the average number of delivered packets (PDR).

4. T= 2 was considered to be the average end-to-end delay of packets containing data.

Phase 2:

Step1: Source node checks for next hop in current routing path.

As shown in following Fig 2. Let S be source and D be destination node. Protocol identifies two possible space regions originated by source. For example, in Fig 2, D is the destination node, S is the source node and A is a black hole. Node S is transferring data packets to node D across the path S, A,B,D. In our scheme, Node S only watches Node A that is the next hop; but doesn't worry for Node 1 and Node 2

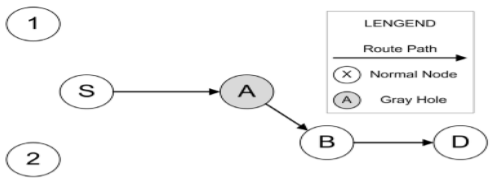

Fig 2: Node Diagram

Step2:
if next hop is suspected node
then goto Step 3
else forward the packets
end

Step3:

Each node should maintain an FPB (Forward Packet Buffer), that is a buffer for packet signatures. The algorithm is split into three parts:

1) When packet is forwarded, it adds its signature to the FPB and overhears the detection node.

Once the action is suggested that the subsequent hop forward the packet, the FPB will release the signature.

3) The detection node should compute the eavesdrop frequency of its next hop over a fixed period of time and compare it to a limit..

The detection node will recognize the subsequent hop as a black or gray hole if the forwarding speed is smaller than the limit. The detection node would later prevent transmitting packets via this suspicious node.

Simulation Setup initial parameters:

Tool	**NS 2.35**
Network	1200 X 1200
Nodes	100
Transmission Range	250 m
CBR (constant bit rate)	512 Byte
Initial energy	8 joules

IV. RESULTS AND DISCUSSION

The simulation of the proposed method against a scenario with the attacks modeled is performed using the network simulator 2.35. In the work done, the author has proposed a new technique for the improvement of selective forwarding attack that is enhanced fuzzy path selection and when the results were compared to the existing Fuzzy Path Selection (FPS) method for the mitigation of selective forwarding attack [14], it was found that the proposed scheme gives better results as shown in the graphs below. **Delay:** The Delay is a very important factor. When network encounter any attack on the ongoing routing path. Then to mitigate the effect of gray and black of attack new routes are established for proper delivery of data. Here, in Fig 3 clearly shows that proposed is performed better than FPS

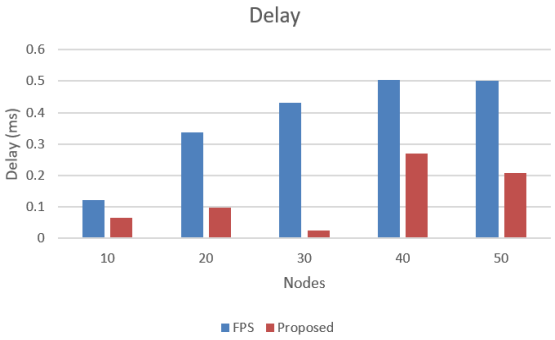

Fig 3. Delay, Existing FPS v/s Proposed

Delivery Ratio: The Delivery ratio is a very important factor. Any network with malicious nodes always decreases the delivery ratio but we can see as mitigation the delivery ratio got improved our proposed protocol is getting higher delivery than FPS in the Fig 4.

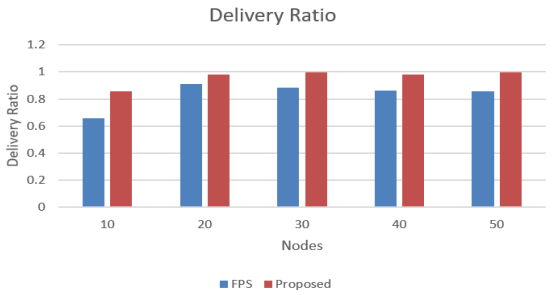

Fig 4. Delivery Ratio, FPS v/s Proposed

Throughput: This is the amount of data packets passed on from a start node to a goal node for each unit of time. The Fig 5 shows the throughput achieved by both routing protocols. The throughput is improved as compared to FPS. The result clearly shows that throughput achieved in our proposed protocol is better in comparison to others. With increasing number of nodes the value of throughput is also increasing.

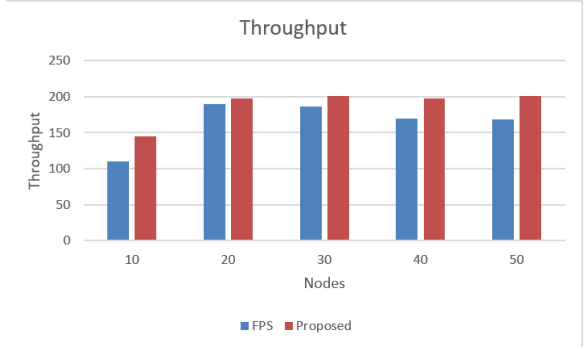

Fig 5. Throughput, FPS v/s Proposed

Dead Nodes: We can see that number of Dead nodes are decreased in proposed with comparison with FPS which describes the network lifetime improved in proposed. Fig 6 clearly shows that with the enhancements in mitigation process of malicious nodes we can able to improve network lifetime 15%.

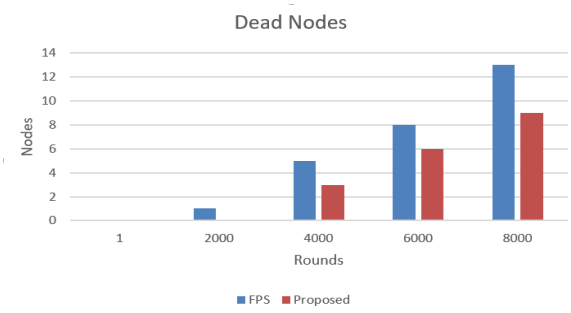

Fig 6. Dead Nodes, Existing FPS v/s Proposed

V. CONCLUSION

WSNs are vulnerable to many kinds of attacks as they serve up as an open network with restricted node resources. Also, owing to the open and dispersed character of the networks and the restricted resources of the nodes, they are also extremely vulnerable to attacks From the above work done, we can conclude that to mitigate the selective forwarding attacks in nodes in Wireless sensor Networks, the proposed enhanced FPS outsources the existing Fuzzy Path selection in terms of throughput, delay, delivery ratio and dead nodes.

REFERENCES

1. Stehlik, Martin, Vashek Matyas, and Andriy Stetsko. "Towards better selective forwarding and delay attacks detection in wireless sensor networks." In 2016 IEEE 13th International Conference on Networking, Sensing, and Control (ICNSC), pp. 1-6. IEEE, 2016.
2. Akyildiz, W. Su, Y. Sankara subramaniam, E. Cayirci, "Wirelss sensor networks: A survey," Computer Networks, 38(4):393-422, 2002.
3. Perrig, Adrian, John Stankovic, and David Wagner. "Security in wireless sensor networks." (2004): 53-57
4. Li, Fengyun, Guiran Chang, Fuxiang Gao, and Lan Yao. "A novel cooperation mechanism to enforce security in wireless sensor networks." In 2011 Fifth International Conference on Genetic and Evolutionary Computing, pp. 341-344. IEEE, 2011.
5. Walters, John Paul, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary. "Wireless sensor network security: A survey." Security in distributed, grid, mobile, and pervasive computing 1 (2007): 367.
6. Karlof, Chris, and David Wagner. "Secure routing in wireless sensor networks: Attacks and countermeasures." In Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications,2003., pp. 113-127. IEEE, 2003.
7. Malik, Rajat, Harkesh Sehrawat, and Yudhvir Singh. "Comprehensive Study of Selective Forwarding Attack in Wireless Sensor Networks." International Journal of Advanced Research in Computer Science 8, no. 5 (2017).
8. Lee, Suk-Bok, and Yoon-Hwa Choi. "A resilient packet-forwarding scheme against maliciously packet-dropping nodes in sensor networks." In Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks, pp. 59-70. ACM, 2006.
9. Xiao, Bin, Bo Yu, and Chuanshan Gao. "CHEMAS: Identify suspect nodes in selective forwarding attacks." Journal of Parallel and Distributed Computing 67, no. 11 (2007): 1218-1230.
10. Zhang, Yuanyuan, and Marine Minier. "Selective forwarding attacks against data and ack flows in network coding and countermeasures." Journal of Computer Networks and Communications 2012 (2012).
11. Ren, Ju, Yaoxue Zhang, Kuan Zhang, and Xuemin Shen. "Adaptive and channel-aware detection of selective forwarding attacks in wireless sensor networks." IEEE Transactions on Wireless Communications 15, no. 5 (2016): 3718-3731.
12. Stehlik, Martin, Vashek Matyas, and Andriy Stetsko. "Towards better selective forwarding and delay attacks detection in wireless sensor networks." In 2016 IEEE 13th International Conference on Networking, Sensing, and Control (ICNSC), pp. 1-6. IEEE, 2016.
13. Shinde, Meghana, and D. C. Mehetre. "Black Hole and Selective Forwarding Attack Detection and Prevention in WSN." In 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), pp. 1-6. IEEE, 2017.
14. Seyyit Alper Sert, Carol Fung, Roy George, and Adnan Yazici. "An efficient fuzzy path selection approach to mitigate selective forwarding attacks in wireless sensor networks." In 2017 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), pp. 1-6. IEEE, 2017.
15. Shila, Devu Manikantan, Yu Cheng, and Tricha Anjali. "Mitigating selective forwarding attacks with a channel-aware approach in WMNs." IEEE transactions on wireless communications 9, no. 5 (2010): 1661-1675.
16. Bysani, Leela Krishna, and Ashok Kumar Turuk. "A survey on selective forwarding attack in wireless sensor networks." In 2011 International Conference on Devices and Communications (ICDeCom), pp. 1-5. IEEE, 2011.
17. Cho, Youngho, and Gang Qu. "Detection and prevention of selective forwarding-based denial-of-service attacks in WSNs." International Journal of Distributed Sensor Networks9, no. 8 (2013): 205920.

18. Djahel, Soufiene, Farid Nait-Abdesselam, and Zonghua Zhang. "Mitigating packet dropping problem in mobile ad hoc networks: Proposals and challenges." IEEE communications surveys & tutorials 13, no. 4 (2010): 658-672.

AUTHORS PROFILE

Deepak N.Biradar is pursing Ph.D in Wireless Sensor Networks under VTU, Belagavi, from 2015. Currently serving as Assistant professor in the Department of CSE at Lingaraj Appa Engineering College from 2011 to till Date. His area of interest is Wireless Sensor Networks, Fuzzy Logic.

Dr. T.S. Vishanath is presently working as Professor in the dept. of ECE, BKIT Bhalki, Karnataka. Affiliated under VTU Belagavi. The author has published many papers in the area of signal processing, image processing and Sensor Networks. The author is a fellow member of ISTE, IETE, IEI. And life member of IJEEE.