IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-6, Issue-11, Nov 2018 E-ISSN: 2347-2693

Detection and Isolation of Malicious Nodes for Selective Forwarding Attack in Wireless Sensor Network

Reenu[1*], Amarvir Singh[2]

[1]Dept. of Computer Science, Punjabi University, Patiala, Punjab, India
[2]Dept. of Computer Science, Punjabi University, Patiala, Punjab, India

[*]Corresponding Author: reenusoni18@gmail.com, Tel.: +91-94649-17329

Available online at: www.ijcseonline.org

Accepted: 20/Nov/2018, Published: 30/Nov/2018

***Abstract*—** A wireless sensor network includes incalculable number of nodes spread over a specific region, where we have to deal with the movements proceeding there. A sensor center, generally, contains sensors, actuators, memory, a processor and they do have correspondence limit. These sorts of networks are much feeble against security attacks. Numerous sorts of dynamic and detached attacks are possible in the sensor network. Among all the possible dynamic attacks, selective forwarding attack is the most generally perceived and ruinous attack. This attack degrades network execution and prompts denial of service attack. The malicious hub activates the attack, which is accessible in the network. In this work, a novel technique has been proposed to perceive and withdraw malicious nodes from the network, which is responsible for triggering the attack. The proposed technique depends on the threshold technique for recognition of malicious nodes. The exploratory outcomes will exhibit that proposed methodology distinguishes and separate the malicious nodes from the network capably. It will upgrade network adequacy to the extent package adversity, concede and grow throughput of the network. NS2 simulator instrument will be used as a piece of it.

***Keywords*—**Wireless, Sensor Network, Sink Node, Sensor Node, Blackhole Attack, Denial of Service Attack, Selective Forwarding Attack, Collision Attack, Man-In-The-Middle Attack, Misdirection Attack, Node Replication Attack, Wormhole Attack.

I. Introduction

Wireless Sensor Network is a mix of little lightweight wireless sensors with figuring components. Wireless sensor networks screen the framework or surroundings by estimating physical parameters. WSNs are most fitting for applications like normal life checking, military request, wise exchanges, current quality control, and impression of fundamental bases, splendid structures, flowed apply self-rule, development watching, investigating human pulses and so forth [2]. Along these lines, Wireless Sensor Network is an accumulation of little gadgets, which gives:

1. The capacity to gauge physical and natural conditions, for example, temperature, weight, and mugginess.
2. The capacity to work gadgets, for example, actuators, engines, and switches that control conditions.
3. Efficient and reliable correspondences.

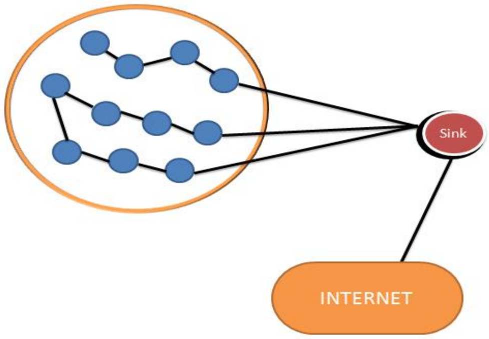


Figure 1.1 Wireless Sensor Network

A. Sensor Node

It collects or sense the data from environment and transmit it to the sink node through multiple hops. Sensor nodes use battery power as an energy source.

B. Sink Node

It performs data aggregation or data agglomeration i.e. it process the data and transmit it. The sink node can use that data locally or globally using the internet.

C. Communication Between Sensor Nodes & Sink Nodes

The development in Wireless Sensor Network depends upon various questions made per Meantime. The sink node transmits the information to be recognized by sending an inquiry all through the sensor field. The sensor nodes respond to the question by get-together the information using their sensors. Finally when the sensor nodes have the outcome of the imbued inquiry will reply to the sink node through some coordinating tradition. A sensor node moreover adds up to the responses to a singular response which saves a portion of the packets to send back to the sink node.

II. SECURITY IN WIRELESS SENSOR NETWORK

Wireless sensor networks are normally introduced at unprotected and severe situations, where security is a fundamental issue. In such unprotected conditions, wireless sensor networks are available to numerous physical and additionally consistent attacks. Security of Wireless sensor network is vital in that capacity kinds of systems are for the most part causing cautions which require sudden consideration. False cautions produced by the wireless sensor network may prompt undesirable activities.

A. Attacks in Wireless Sensor Network

- **Wormhole Attack**
  In this, a malicious node, records packets at a specific area in the network and tunnel them to another area. At the point when the control messages are steering and are burrowed it makes disturbance. It is a network layer attack. The answer for this issue is checking the network and adaptable steering plans.
- **Blackhole Attack**
  In this attack, malicious node catches and reinvents an arrangement of nodes in the network and hinders the packets that are gotten as opposed to sending them towards the base station. Any packet that goes into the black hole locale is caught by the malicious node and never achieves the destination node. [7, 8]
- **Denial of Service Attack**
  The malicious node in this attack hits on the availability of a node and every single other node in the entire of the network. The aim of this attack is to obstruct the administrations of the sensor nodes [7, 8]. The attacker for the most part utilizes battery retention technique and radio signal jamming.
- **Selective Forwarding Attack**
  In this attack, the malicious node fills in as a typical node yet declines to forward certain chose parcels and essentially drop them. This Attack likewise carries on like a Blackhole Attack in which it declines to forward each packet. It might likewise carry on like a Misdirection Attack may forward the messages to the wrong way [24, 25].
- **Collision Attack**
  In this attack, an attacker endeavors to send the information on a similar recurrence with which different nodes are transmitting the data, so the packets impact and retransmission is required [24].
- **Man-In-The-Middle Attack**
  In this attack, an attacker sits in the middle of the sender and the collector node. The data being passed by the sender is caught by the attacker sitting in the center. In a few occasions, an attacker may take on the appearance of the first sender to speak with the receiver or take on the appearance of the collector to answer to the sender.
- **Misdirection Attack**
  The substance packet is directed to an unexpected goal in comparison to the first place in this sort of attack. The attacker does the misguidance of the packet here. The network will corrupt because of the expansion in time in which the packet ought to be gotten. There is a nearness of the narrow-minded nodes in the network, which mislead the packets, and there is a decline in the productivity of the total framework because of this. [1], [2], [7], [8].
- **Node Replication Attack**
  The attacker endeavours to include a malicious node in the network by appointing the malicious node a similar Node ID of some current node in the node [14].

III. LITERATURE SURVEY AND KEY PAPER

Saqib Ali et al. [1] provided classification of layer-to-layer, outside and interior attacks to wireless sensor network and cyber-physical system. Notwithstanding that, the part distinguishes the known security location and conceivable methodologies against the dangers for wireless sensor systems and cyber physical system. At long last, an examination of ways to deal with protects wireless sensor network and cyber physical system against such attacks is displayed.

G. Padmavathi et al. [2] presented the security objectives for sensor networks, different attacks in wireless sensor networks and the security instrument identified with various attacks. The paper additionally exhibited the difficulties of sensor networks.

Roshan Singh Sachan et al. [5] displayed there are a considerable measure of examples that have been happening in which the recognition of the attack of DoS and misdirection attacks has not been possible. An algorithm is proposed which will give assistance to the help with throughput and delay of the packets. Better execution is seen in the tree network topology than in the mesh topology network.

Bharat Bhushan et al. [7] analyzed the security threats and vulnerabilities forced by the particular open nature of WSNs. Next, paper investigate the potential security threats at various protocol layers. Here different security attacks are distinguished alongside their countermeasures that were examined by various specialists as of late. We additionally give a detailed review of data aggregation and the energy-efficient routing protocols for WSNS.

Hero Modares et al. [11] proposed an overview of the security issues, security standards. The paper represented the distinctive security attacks and showed the diverse cryptographic techniques.

Ruchita Dhulkar et al. [12] has depicted about the security of the wireless sensor networks. There are numerous attacks, which are perilous for the execution of the network like a black hole, wormhole and so forth. Misdirection is most hazardous routing attacks network. In this paper, they proposed a strategy to identify malicious node to work network member in the data routing.

Sachan RS et al. [20] proposed strategy depends on node localization, in which delay per hop is checked and the node which is expanding delay mostly which can be distinguished as a malicious node.

Padmavathi DG et al. [21] presented one of the real difficulties wireless sensor networks confront today is security. While the deploying of sensor nodes in an unattended domain. The wireless communication innovation likewise procures different sorts of security dangers. This paper examines a wide assortment of attacks in WSN and their characterization.

Liangmin et al. [24] presented the malicious nodes may specifically drop some significant data packets, which truly pulverize the network's data gathering and reduction the accessibility of sensor services. In this paper, we present a lightweight resistance conspire against selective forwarding attacks.

Baviskar BR at al. [26] proposed a productive strategy that uses different base stations conveyed in the network to check the effect of black holes on data transmission, utilizing java simulator and performance contrast and numerous base station and without various base station to forestall black hole attacks.

IV. Research Methodology

An active attack that is responsible for dropping the data and control packets within the network is known as the selective forwarding attack. There is a minimization of performance of network in terms of various parameters when a malicious node is present within the network. The parameters such as energy consumption, throughput and delay define the performance of the network, which can change as per the modifications made within the network.

In this work, in order to recognize and remove the malicious nodes from the network, a technique has been proposed. On the basis of traffic analyzer and threshold values present within the network, there is a technique proposed.

V. Proposed Mythology

Input: Sensor nodes
Output: Detection of malicious nodes

```
1.    Deploy the wireless sensor node with the finite number of sensor nodes
2.    Select Central node ()
      For (i=0;i=n;i++)
          No.pkts=node(i)
          If (node(np.pkts(i)> np.pkts(i+1)))
          Central node=node(i)
      End
3.    Each node register with the central node with their IP and MAC address
4.    Assign Bandwidth ()
      For (i=0;i=n;i++)
              Bandwidth node(i+1)=total
          bandwidth-bandwidth node(i+1)
      End
5.    Central controller node check the sensor nodes randomly
          if (node(bandwidth use=bandwidth
      assigned)
              if( Node(throughput < threshold
          throughput)
              malicious =Node(i)
6.    Repeat step 2 to 5 until malicious node get detected
```

A. *Proposed Framework*

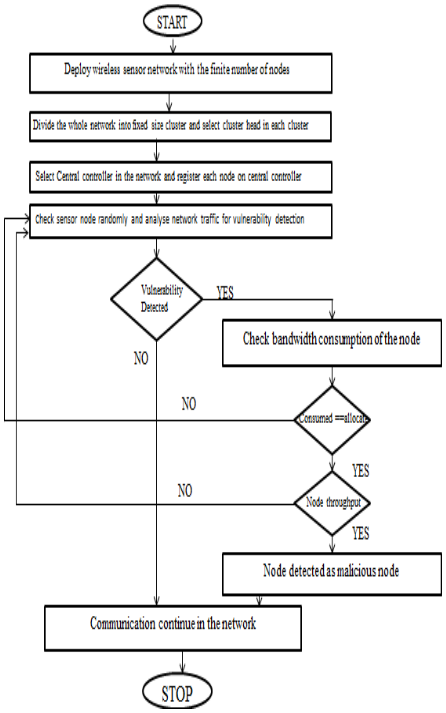

START
Deploy wireless sensor network with the finite number of nodes
Divide the whole network into fixed size cluster and select cluster head in each cluster
Select Central controller in the network and register each node on central controller
Check sensor node randomly and analyse network traffic for vulnerability detection
Vulnerability Detected
YES
NO
Check bandwidth consumption of the node
NO
Consumed ==allocat
YES
NO
Node throughput
YES
Node detected as malicious node
Communication continue in the network
STOP

Figure 5.1 Flow of Work for detecting malicious node

B. Process and Flow

Step 1: Deploy the wireless sensor node with the finite number of sensor nodes.

Step 2: The whole network is divided into fixed size clusters. The location based clustering is applied to cluster the whole network. The cluster heads are selected on the basis of distance and energy. The nodes in the cluster will aggregate its data to the cluster head.

Step 3: Base station is selected. The required data will be transmitted to a base station by the cluster head.

Step 4: Check sensor nodes randomly, and analyze network traffic for vulnerability detection

Step 5: Decision-making process starts for vulnerability detection, if vulnerability is not detected; control passes to the communication continue and stop. If vulnerability is detected, bandwidth is computed.

Step 6: If bandwidth consumption is not equal to the allocated, control passes to the step 4, otherwise node throughput is calculated.

Step 7: If node throughput is not calculated, control passes to the step 4, otherwise node is detected as malicious node and communication continue in the network.

VI. RESULTS AND DISCUSSIONS

To examine the execution of the model, it is made to be performed inside a simulation. It is an open-source event driven test system designed particularly for research in computer communication systems. NS2 comprises of two key languages: C++ and Object-oriented Tool Command Language (OTcl).C++ characterizes the inner system of the recreation objects. OTcl sets up re-enactment by gathering and designing the articles and in addition booking discrete events. The C++ and the OTcl are connected together utilizing TclCL.

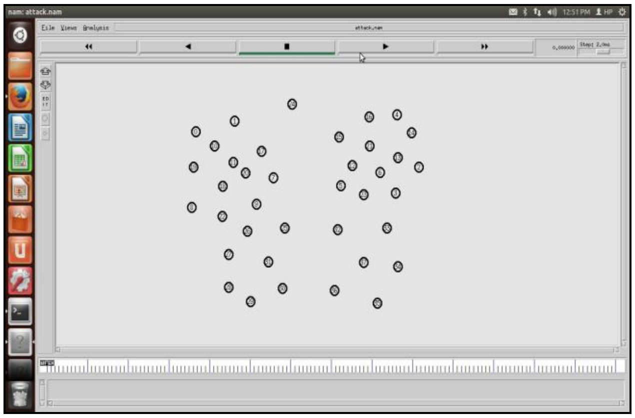
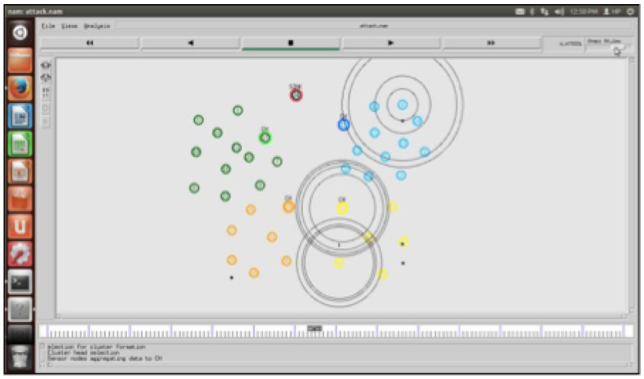


Figure 6.1 Network Deployments

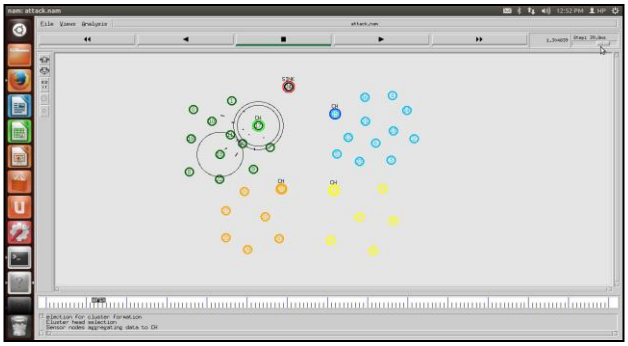
Figure 6.1 presents the network is deployed with the finite number of sensor nodes. The whole network is divided into fixed size clusters. The location based clustering is applied to cluster the whole network.



```
election for cluster formation
Cluster head selection
Sensor nodes aggregating data to CH
```

Figure 6.2 Clustering

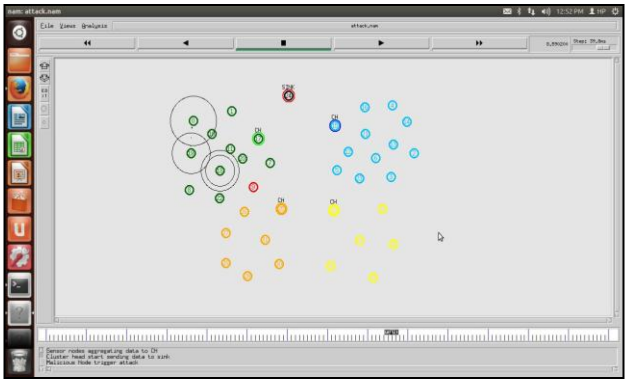
Figure 6.2 presents the whole network is divided into fixed size clusters. The location based clustering is applied to cluster the whole network. The LEACH protocol is applied to select cluster head in each cluster, the cluster heads are selected on the basis of distance and energy.



```
election for cluster formation
Cluster head selection
Sensor nodes aggregating data to CH
```

Figure 6.3 Data Aggregation

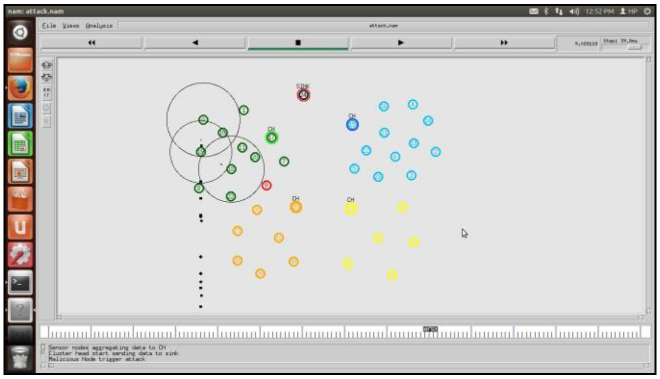
Figure 6.3 presents the nodes in the cluster will aggregate its data to the cluster head. The required data will be transmitted to a base station by the cluster head.



```
Sensor nodes aggregating data to CH
Cluster head start sending data to sink
Malicious Node trigger attack
```

Figure 6.4 Trigger Attack

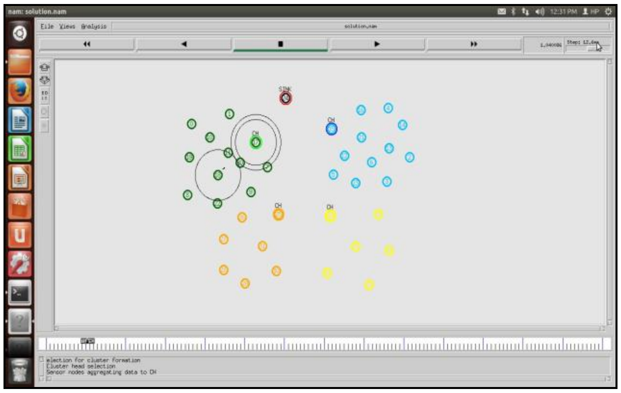
Figure 6.4 presents the shortest path will be established from cluster head to cluster head. In the established path, the malicious node exists which is responsible for triggering selective forwarding attack in the network.



Sensor nodes aggregating data to CH
Cluster head start sending data to sink
Malicious Node trigger attack

Figure 6.5 Trigger Attack

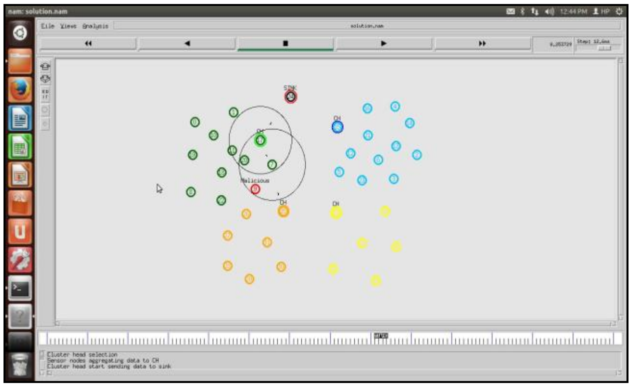
Figure 6.5 presents the selective forwarding attack is triggered within the network for establishing the path, which is mainly due to the malicious node.



election for cluster formation
Cluster head selection
Sensor nodes aggregating data to CH

Figure 6.6 Delay Per Hop

Figure 6.6 presents there are some malicious nodes present within the network that result in causing the misdirection attack. The delay per hop is computed for separating the malicious node from the network.



Cluster head selection
Sensor nodes aggregating data to CH
Cluster head start sending data to sink

Figure 6.7 Malicious Node Isolation

Figure 6.7 presents the delay per hop is counted from the base station within this figure. The malicious node is isolated from the network in this complete scenario.

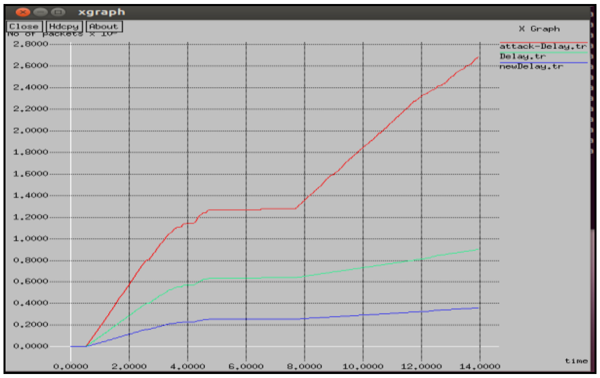


Figure 6.8 Delay Graph

Figure 6.8 presents the delay parameters, there is a comparison made amongst the LEACH, the attack as well as the proposed technique. There is maximum delay caused during the presence of attacks. There is least delay within the proposed method as there is no attack present in that network.

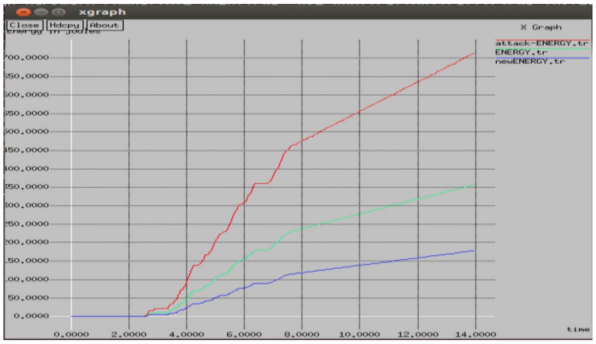


Figure 6.9 Energy Graph

Figure 6.9 presents the comparison of the proposed; attack scenario is shown in terms of energy. It is been analyzed that energy consumption of the proposed scenario is least as compared to attack scenario.

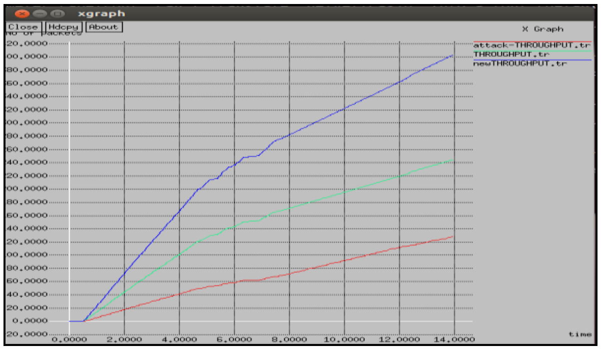


Figure 6.10 Throughput Graph

Figure 6.10 presents the comparison has been made for the attack and the proposed method in terms of throughput. In comparison to the other methods, the throughput of proposed method is the highest.

VII. Conclusion And Future Scope

The networks that can sense the environmental conditions with the help of sensor nodes present within them are known as wireless sensor networks. The sensed information is gathered and passed further. The lifetime of the sensor nodes is very less because the size of battery available within them is very less. The malicious nodes can enter within the wireless sensor networks mainly due to the self-configuring nature of these networks. There can be various attacks possible within the network due to the presence of malicious nodes within the network. Amongst these attacks is the selective forwarding attack. The technique is proposed in this paper, which can identify and separate the malicious nodes from the network. On the basis of threshold mechanisms the base station analyzed the delay per hop within the network. The malicious node is identified on the basis of the delay such that the node that contributes maximum delay will be recognized as malicious node. This helps in minimizing the energy consumption of the network along with the increment in throughput and reduction of delay within the network. In future, proposed technique can be applied in detecting and isolation of malicious nodes, which causes the Denial-of-Service attack in wireless sensor network scenario.

VIII. References

[1] Ali, S., Al Balushi, T., Nadir, Z., & Hussain, O. K. (2018). WSN Security Mechanisms for CPS. In Cyber Security for Cyber Physical Systems (pp. 65-87). Springer, Cham.

[2] Padmavathi, D. G., & Shanmugapriya, M. (2009). A survey of attacks, security mechanisms and challenges in wireless sensor networks. arXiv preprint arXiv:0909.0576.

[3] Raghunandan, G. H., & Lakshmi, B. N. (2011, February). A comparative analysis of routing techniques for Wireless Sensor Networks. In Innovations in Emerging Technology (NCOIET), 2011 National Conference on (pp. 17-22). IEEE.

[4] younis Abdullah, M., Hua, G. W., & Alsharabi, N. (2008, June). Wireless sensor networks misdirection attacker challenges and solutions. In Information and Automation, 2008. ICIA 2008. International Conference on (pp. 369-373). IEEE.

[5] Sachan, R. S., Wazid, M., Singh, D. P., Katal, A., & Goudar, R. H. (2013, January). Misdirection attack in WSN: Topological analysis and an algorithm for delay and throughput prediction. In Intelligent Systems and Control (ISCO), 2013 7th International Conference on (pp. 427-432). IEEE.

[6] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: a survey. Computer networks, 38(4), 393-422.

[7] Bhushan, B., & Sahoo, G. (2018). Recent Advances in Attacks, Technical Challenges, Vulnerabilities and Their Countermeasures in Wireless Sensor Networks. Wireless Personal Communications, 98(2), 2037-2077.

[8] Sharma, K., & Ghose, M. K. (2010). Wireless sensor networks: An overview on its security threats. IJCA, Special Issue on “Mobile Ad-hoc Networks” MANETs, 42-45.

[9] Sachan, R. S., Wazid, M., Singh, D. P., & Goudar, R. H. (2013, April). A cluster based intrusion detection and prevention technique for misdirection attack inside WSN. In Communications and Signal Processing (ICCSP), 2013 International Conference on (pp. 795-801). IEEE.

[10] Rani, L., & Rani, E. V. A Novel Study on Data Flow Routing with Energy Optimization under Different Attacks in WSN.

[11] Modares, H., Salleh, R., & Moravejosharieh, A. (2011, September). Overview of security issues in wireless sensor networks. In 2011 Third International Conference on Computational Intelligence, Modelling & Simulation (pp. 308-311). IEEE.

[12] Dhulkar, R., Pokharkar, A., & Pise, M. R. (2015). Survey on different attacks in Wireless Sensor Networks and their prevention system.

[13] Jadidoleslamy, H. (2011). A hierarchical intrusion detection architecture for wireless sensor networks. International Journal of Network Security & Its Applications, 3(5), 131.

[14] Wang, C. H., & Li, Y. T. (2013, July). Active black holes detection in ad-hoc wireless networks. In Ubiquitous and Future Networks (ICUFN), 2013 Fifth International Conference on (pp. 94-99). IEEE.

[15] Lupu, T. G., Rudas, I., Demiralp, M., & Mastorakis, N. (2009, September). Main types of attacks in wireless sensor networks. In WSEAS international conference. proceedings. recent advances in computer engineering (No. 9). WSEAS.

[16] Singh, V. P., Jain, S., & Singhai, J. (2010). Hello flood attack and its countermeasures in wireless sensor networks. International Journal of Computer Science Issues (IJCSI), 7(3), 23.

[17] Zhang, Y. Y., Li, X. Z., & Liu, Y. A. (2012). The detection and defence of DoS attack for wireless sensor network. The journal of china universities of posts and telecommunications, 19, 52-56.

[18] Tan, H., Ostry, D., Zic, J., & Jha, S. (2013). A confidential and DoS-resistant multi-hop code dissemination protocol for wireless sensor networks. Computers & Security, 32, 36-55.

[19] Zhan, G., Shi, W., & Deng, J. (2010, February). Tarf: A trust-aware routing framework for wireless sensor networks. In European Conference on Wireless Sensor Networks (pp. 65-80). Springer, Berlin, Heidelberg.

[20] Sachan, R. S., Wazid, M., Singh, D. P., & Goudar, R. H. (2013, April). A cluster based intrusion detection and prevention technique for misdirection attack inside WSN. In Communications and Signal Processing (ICCSP), 2013 International Conference on (pp. 795-801). IEEE.

[21] Padmavathi, D. G., & Shanmugapriya, M. (2009). A survey of attacks, security mechanisms and challenges in wireless sensor networks. arXiv preprint arXiv:0909.0576.

[22] Sharma, K., & Ghose, M. K. (2010). Wireless sensor networks: An overview on its security threats. IJCA, Special Issue on “Mobile Ad-hoc Networks” MANETs, 42-45.

[23] Lv, S., Wang, X., Zhao, X., & Zhou, X. (2008, December). Detecting the sybil attack cooperatively in wireless sensor networks. In Computational Intelligence and Security, 2008. CIS'08. International Conference on (Vol. 1, pp. 442-446). IEEE.

[24] Xin-Sheng, W., Yong-Zhao, Z., Shu-ming, X., & Liang-min, W. (2009, October). Lightweight defense scheme against selective forwarding attacks in wireless sensor networks. In Cyber-Enabled Distributed Computing and Knowledge Discovery, 2009. CyberC'09. International Conference on (pp. 226-232). IEEE.

[25] Kaplantzis, S., Shilton, A., Mani, N., & Sekercioglu, Y. A. (2007, December). Detecting selective forwarding attacks in wireless sensor networks using support vector machines. In Intelligent Sensors, Sensor Networks and Information, 2007. ISSNIP 2007. 3rd International Conference on (pp. 335-340). IEEE.

[26] Baviskar, B. R., & Patil, V. N. (2014). Black hole Attacks mitigation and prevention in wireless sensor network. International Journal of Innovative Research in Advanced Engineering (IJIRAE), 1(4), 167-169.

[27] Wang, C. H., & Li, Y. T. (2013, July). Active black holes detection in ad-hoc wireless networks. In Ubiquitous and Future Networks (ICUFN), 2013 Fifth International Conference on (pp. 94-99). IEEE.

[28] Mishra, A., Nadkarni, K., & Patcha, A. (2004). Intrusion detection in wireless ad hoc networks. IEEE wireless communications, 11(1), 48-60.

[29] young Kim, J., Caytiles, R. D., & Kim, K. J. (2012). A review of the vulnerabilities and attacks for wireless sensor networks. 9(3), 241-250.

[30] Sharma, K., & Ghose, M. K. (2010). Wireless sensor networks: An overview on its security threats. IJCA, Special Issue on “Mobile Ad-hoc Networks” MANETs, 42-45.

[31] Collins, M., Dobson, S., & Nixon, P. Securing Wireless Sensor Networks: Introducing ASLAN-A Secure Lightweight Architecture for WSNs.

[32] Mohammadi, S., & Jadidoleslamy, H. (2011). A comparison of link layer attacks on wireless sensor networks. arXiv preprint arXiv:1103.5589.

[33] Anand, C., & Gnanamurthy, R. K. (2016). Localized DoS Attack Detection Architecture for Reliable Data Transmission Over Wireless Sensor Network. Wireless Personal Communications, 90(2), 847-859.

[34] Said, O., & Elnashar, A. (2015). Scaling of wireless sensor network intrusion detection probability: 3D sensors, 3D intruders, and 3D environments. EURASIP Journal on Wireless Communications and Networking, 2015(1), 46.

[35] Biswas, S., & Adhikari, S. (2015). A survey of security attacks, defenses and security mechanisms in wireless sensor network. International Journal of Computer Applications, 131(17), 28-35.

Authors Profile

Reenu pursed Bachelor of Computer Application (BCA) from S.B.S.B.M. Govt. College, Sardulgarh (Punjabi University, Patiala) in year 2011. Later she pursed Masters of Computer Application (MCA) from Shah Satnam Ji Institute of Technology & Management, Sirsa (Guru Jambheshwar University, Hisar). She is currently pursuing Mphil. (Computer Science) from Punjabi University, Patiala. Her main research work focuses on Cryptography Algorithms, Network Security & Cloud Security and Privacy.

Amarvir Singh pursed Bachelor of Computer Science and Engineering and Masters in Internet and Communication Technology from Punjabi University Patiala. Pursuing Ph.D. and currently working as Assistant Professor in Department of Computer Science, Punjabi University Patiala, since 2012. He has 5 years of teaching experience and 3 years of Research Experience.