Detection Of Selective Forwarding Attacks Using CHEMAS Technique In Wireless Sensor Networks

**Abstract:** Wireless Sensor Networks (WSNs) consist of distributed autonomous devices that monitors both physical and environmental conditions. Sensor Networks are used for weather prediction and for measuring temperature, sound, wave, vibration, pressure etc. Sensor Networks suffer from various security attacks like (i) sink hole attack, (ii) black hole attack, (iii) wormhole attack and (iv) selective forwarding attacks. Selective forwarding attack happens in compromised nodes by dropping packets selectively. In such attacks, most of the time malicious nodes behave like normal nodes but will from time to time selectively drop sensitive packets, such as a packet reporting the movement of the opposing forces, and thereby make it harder to detect their malicious nature. This paper proposes an efficient checkpoint based multi-hop acknowledgement scheme (CHEMAS) to detect the compromised nodes that perform a selective forwarding attack when sensing data transmission. This paper proposes a more effective alert and alarm message transmission procedure. When an attack is identified, Server stops the process and the packets are retransmitted through the new shortest path without losing the connection. Dijikstra’s shortest path algorithm is used to select the alternate route. Detection scheme employed to identify the malicious node uses both theoretical analysis and simulations. The simulation results indicate that this scheme achieves a high detection rate and improved the communication overhead.

**Keywords:** Wireless Sensor Network, Selective Forwarding Attacks, Compromised Nodes, CHEMAS Technique, Dijistra’s Shortest Path Algorithm.
1. Introduction:

Wireless Sensor Networks (WSNs) is emerging as an important research in the field communication network. Wireless sensor network ranges from sparse networks with 10s of nodes to populated networks with 1000s, possibly 10000s or 100000s of sensors collecting data from the environments. These Wireless Sensor Nodes are tiny devices with limited energy, memory, transmission range, and computational power. WSN is a self-configuring network of small sensor nodes which communicate with each other using radio signals. WSN joins together sensing, computation and communication in a single device called sensor nodes. Wireless Sensor Nodes are also called as motes. In WSN, sensor nodes are used to send packets to a base station with the help of multi-hop transmission. Sensor nodes are classified into clusters and each of these clusters has a cluster head. Through cluster heads, Sensor Nodes communicate data to the base station by combining data from its members [1].

WSN require some amount of security in order to maintain high survivability and integrity of the network. Many emerging and future applications require strong security in order to function acceptably. For military applications, WSNs could be placed behind enemy lines in order to detect and track enemy soldiers and vehicles. In indoor environment, Sensor Networks could be deployed in order to detect intruders and security violations through wireless home security system. In office buildings, Sensor Networks are used in temperature monitoring/regulating, fire alarm systems, manufacturing machinery performance monitoring, building safety, earthquake monitoring and vehicular movement and so on. Due to resource constraints of energy and memory, the conventional security measures are not suitable to these WSNs. An adversary can compromise a sensor node; it alters the integrity of the data, eavesdrops on messages, injects fake messages and waste network resources. Several security attacks exist in Wireless Sensor Networks and they are, Dos attack, Sink hole attack, Black hole attack, Wormhole attack, Selective forwarding attacks, Sybil attacks, Sybil attacks, Node replication attacks, Hello flood attack. This paper focuses on Selective Forwarding Attacks and how to identify malicious node in this attack. To detect malicious node in Selective Forwarding Attack using CHEMAS in WSNs. This technique will improve a higher detection ratio with less communication overhead.

1.1. Selective Forwarding Attack:

The selective forwarding Attack was first described by Karlof and Wagner [3]. Selective Forwarding Attack is a network layer attack [2]. In this type of the attack compromised nodes
drop particular sensitive messages and forward the rest. It is difficult to identify the compromised node in the whole network. Selective forwarding attacks are most effective when the attacker is explicitly included on the path of a data flow. Selective forwarding and black hole attacks are very disastrous attacks for sensor networks if used with sinkhole attack because the intruder can drop most of the important packets. Further classification of this attack is inside attack and outside attack. Inside attack occurs within the network through compromised nodes and outside attack occurs from outside of the network by jamming the communication channels between uncompromised nodes.

This paper is organized as follows: Section 2 present related works and the overview of selective forwarding attacks techniques. Section 3 deals with proposed works on Selective Forwarding Attack detection in WSNs using CHEMAS technique. Section 4 contains simulation results and discussions. Section 5 gives the future research directions. The final section concludes this paper.

2. Related Works:

Various techniques are introduced by several researchers to detect malicious nodes that cause selective forwarding attack in Wireless Sensor Networks. These techniques are classified and depicted below in figure 1[4].
Figure 1: Classification of Selective Forwarding Attacks

2.1. CHEMAS Technique:

CHEMAS was proposed by Bin Xiao et al., to detect selective forwarding attack. When message is generated by a source node and is delivered to the base station, the checkpoint nodes are selected randomly. The base station and each checkpoint nodes generate ACK message that is transmitted from the start node to the source node. ACK messages have the TTL value, which sets the hop count. If TTL becomes zero, ACK message is dropped and an alert message is sent to the source node. If a particular node does not send ACK message to the source then it is identified as the compromised node. Then the source node sends an alarm message about the compromised node to the base station.
Ji Won Kim, et al., [5] have proposed another technique for the CHEMAS to detect the compromised nodes that perform a selective forwarding attack when sensing data transmission. This paper has achieved a higher detection ratio through each checkpoint node and it generates acknowledgement message to confirm the normal packet.

Ji Won Kim, et al., [6] work, have presented a control method of checkpoint node selection using a fuzzy rule system and feedback in the CHEMAS. The sink node and each checkpoint node generate ACK packets to confirm normal packet delivery. If a node has not received sufficient ACK packets, then the nodes generate an alert packet to report the suspect node. Compromised nodes can be detected by analyzing the alert information reported.

2.2. Defense Mechanism:

Defensive technique for selective forwarding attack consists of three phases for secure information delivery. In first phase the node discovers a path and its neighbor nodes, in second phase, data is propagated in multipath, it checks whether the data received is correct or not, and in the final phase if any error is detected then a MONITOR packet is generated and the malicious node is removed.

Pandarinath P., [7] has given defensive technique for selective forwarding attack in localization. This technique utilizes secret sharing of information and this information is shared between source and destination using secret sharing algorithm.

Arpita Parida, et al., [8] have introduced a Defensive technique. If an attack is encountered then a monitor packet is generated and subsequently the malicious node is removed. It finds a new path so that the connection will not to be lost and also good delivery ratio can avoid delays.
2.3. Lightweight Defense Scheme:

Lightweight security scheme is used to detect selective forwarding attack using multi hop acknowledgement technique. This scheme allows both the base station and source nodes to collect attack alarm information from intermediate nodes. In other words, though the base station is deafened by malicious node the source node can make decisions and responses. The scheme can efficiently obtain those alarm information whenever intermediate nodes in a packet forwarding path detect any malicious packet dropping.

Wang Xin-sheng, et al., [9] have proposed a light weight defense scheme against selective forwarding attack which uses neighbor nodes as monitor nodes. The neighbor nodes (monitoring nodes) monitor the transmission of packet drops and resend the dropped packets using a hexagonal WSN mesh topology.

Sultana, et al., [10] have proposed a novel light-weight scheme to securely transmit provenance for sensor data. The proposed technique relies on in-packet Bloom filters to encode provenance. This paper introduces efficient mechanisms for provenance verification and reconstruction at the base station. The proposed technique is evaluated both analytically and empirically, and the results prove its effectiveness and efficiency for secure provenance encoding and decoding.

2.4. Watermark Technology:

The digital watermarking technology is used to calculate the rate of packets of dropped and modified. Each sensor node can send only a few bits at a time and so the length of watermark embedded into the data should be very short. The source node generates the watermark W with key K and the feature of the original data. Then the source node embeds the watermark into the original data and transfers it through the media. When the packets reach the Base Station, the Base Station obtains the feature of the packets and generates the watermark W1 by watermark generation algorithm, then the Base Station extracts the watermark directly from the received packets by Watermark embedding algorithm denoted as W2; finally the packet modified rate is calculate by comparing the W1 and W2.

Deng-yin ZHANGa, et al., [11] have presented a technique based on digital watermarking technology. This method embeds watermark into the source data packets, and extract them at the base station without any packet loss. The malicious node prevented from dropping the data.
Baowei Wang, et al., [12] have proposed a novel multiple watermarking method called Multi-mark. This technique provides privacy, security, and saved storage space and the amount of data transmitted. Multi-mark is a network structure-free scheme, which can be easily and efficiently applied to the resource limited sensor networks.

3. Selective Forwarding Attack Detection In WSN Using CHEMAS Technique:

This thesis proposes a CHEMAS technique against selective forwarding attack. This scheme uses a multi level dynamic tree routing for forwarding the packets to the sink node. A simple approach to detect packet loss is acknowledgement. In case of packet drop, source resends the packet through alternate path. Dijistra’s shortest path algorithm used to find the alternate path. This makes scheme more secure and reliable in presence of malicious nodes. Selective forwarding attack means the malicious nodes drop or modify packets selectively, so that the information can't be transferred to the BS completely. When the BS detects that there is malicious node in the transmission path, it will start the malicious node mechanism to find the malicious nodes. The detection mechanism is as follows:

Step 1 - Source node transfers the packets to the destination through different paths.

Step 2 - Each and every node sends acknowledgement to the previous node. A simple approach to detect packet loss is acknowledgement; it shows that there is a malicious node in the transmission path. If any node does not send acknowledgement it shows that the previous node is malicious node.

Step 3 - Then the current node sends an alert message to inform the Source node about the details of malicious node. When an attack is identified Server Stops the process and Source node sends an alarm message to the destination.

Step 4 - Source node retransmits the packet through new shortest path without losing the connection.

Step 5 - The alternative path is chosen based on Dijikstra’s shortest path algorithm.
4. Results And Discussions:

4.1. Simulation Environment:

Simulate the proposed CHEMAS Technique to evaluate the efficiency. The simulation experiment in NS2 shows the great efficiency of the algorithm and related network performance. In this simulation, the network configurations are as follow: the area coverage is 25x25 m², where 25 nodes have been deployed randomly. In the network, there are 2 source node and a BS node. The hops between BS and source node assign randomly. The different malicious behaviors and network environments will be set by the Error Model in NS2. In simulation experiments, place 2 malicious nodes around source node. Source node sends 50 bits collection data every time. Group length (M) is 8 bit. The packet loss rate R is 0.1 in normal network, so we set R=0.1 as the threshold. Perform the experiment 2 times and then take mean detection rate of malicious node. The following is malicious node detection rate which is detected in different network environments and different malicious behaviors.

4.1.1. Packet Delivery Ratio In The Presence Of One Malicious Node:

Behavior of the system is observed when malicious node is inserted in WSNs.

![Graph](image)

*Figure 3: Packet delivery ratio in presence of one malicious node*

4.1.2. Packet Delivery Ratio In The Presence Of Two Malicious Nodes:

Here two malicious nodes are inserted in a wireless sensor network. Then the packet delivery ratio is compared in different rounds to find out the behavior of the system.
4.1.3. Comparison Between Existing And Proposed Scheme:

Figure 4.1.2 shows the detection accuracy, the number of misidentification of non-compromised node as a suspicious node is increased, the detection accuracy is lower than the original communication scheme. In proposed scheme, packets are retransmitted through new path so packet delivery ratio is increased compare with existing scheme. Figure 4.3.3 shows that packet throughput for proposed scheme.

Figure 5: Comparison of Detection accuracy
Packet delivery ratio is the ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination. Packet delay is the delay in retransmission of the failed packet to destination. Throughput is defined as the number of successfully delivered bits in their dedicated transmission duration. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

Figure 6: Packet Throughput of Bits Successfully Delivered to the Destination
5. Future Research Directions:

In this work, a single static path is created for sending packets to the sink node in the network. When an attack is identified, server removes the malicious node and the packets are retransmitted through the new shortest path without losing the connection. This technique can be further enhanced by hiding the packets using the secret sharing algorithm. This approach leads to less conception of energy, good delivery ratio and avoids delays.

6. Conclusion:

This paper, propose a simple and efficient security scheme for detecting selective forwarding attacks. In this original method, a very large amount of alert and alarm message is used to identify the compromised nodes. CHEMAS technique is very effective technique for malicious node detection to compare with any other techniques. The detection mechanism will be activated only when there malicious attacks exist in the network In CHEMAS, the selection probability of checkpoint is an important factor to determine the security intensity and energy efficiency. The proposed method enhances detection ratio with similar energy consumption to the original CHEMAS scheme. The simulation experiment in NS2 shows the great efficiency of the algorithm and related network performance.
References:


