S.V. Annlin Jeba  
Assistant professor,  
Department of CSE  
CSI Institute of Technology,  
Thovalai, Tamilnadu, India  
anlin_jeba@yahoo.co.in

Dr. B. Paramasivan  
Professor and Head  
Department of CSE  
National Engineering College,  
Kovilpatti, Tamilnadu, India  
bparamasivan@yahoo.com

ABSTRACT

Wireless sensor networking is an emerging technology, which supports many emerging applications due to their low cost, small size and untethered communication over short distances. Sensor nodes are deployed in open hostile environment in WSN applications. An adversary can easily compromise sensor nodes due to their unattended nature. Adversaries can inject false data reports into the WSN through compromised nodes. The false data reports lead the en-route nodes and the base station to make false decision. False decision depletes the energy of en-route nodes and the base station. Hence create threat to the lifetime of the sensor nodes. To detect and drop false data, number of en-route filtering schemes have been developed. This paper review some of the existing en-route filtering schemes and analyses the performance of those en-route filtering schemes based on their filtering efficiency. Finally a case study about some of the en-route filtering scheme is provided and this provided the aspects for the designers to implement suitable scheme to defend against false data injection attack.

Keywords: compromisation, en-route filtering, false data, attack, sensor node

1. INTRODUCTION

A Wireless Sensor Network (WSN) is composed of a large number of small sensor nodes having limited computation capacity, restricted memory space, limited power resource and short-range of communication[1][2]. WSN has one or more base-station which does the functions of calculation and decision-making and can be compared with the functionalities of server or in some cases as a gateway in a computer network. In WSN applications sensor nodes are deployed in hostile environment [3][4]. In such environment sensor nodes are subjected to various types of attacks such as eavesdropping, masquerade, false data injection, selective forwarding. An adversary can mount such attacks from outside as well as inside the network. Sensor nodes sense the events that occur in their surrounding environment. Generate event report for the sensed information and the event report has to
be send to the base station through the en-route nodes. When event report is forwarded through en-route node a compromised node can forge the report. False data contain false information from compromised nodes [5]. This false data injection attack depletes the energy of the en-route nodes. This may be dangerous in scenarios such as battlefield surveillance and environmental monitoring by making false decision. Moreover, it is a difficult task to monitor all the sensor nodes in the field of interest.

Though several recent research efforts have proposed mechanisms to enable node and message authentication in sensor networks, those proposed solutions can only prevent false reports injection by outside attackers. They are made ineffective when any single node is compromised. One solution to reduce the impact of false data injection into the network through a compromised node is to filter the false data by the en-route node as early as possible before reaching the base station. Authentic and accurate data is provided to surrounding sensor node and to the sink through en-route filtering scheme. En-route filtering is an effective way to defeat false data injection attacks. Moreover, in en-route filtering schemes not only the destination node but also the intermediate nodes can check the authenticity of the message in order to reduce the number of hops or nodes the false message travels. This paper describes about many of the existing en-route filtering schemes. In addition analyze about the advantages and disadvantages of the related en-route filtering scheme.

2. COMMON SECURITY THREATS ON WSN

An attack is an event that diminishes or eliminates a network's capacity to perform its expected function and an adversary is a person or another entity that attempts to cause harm to the network by unauthorized access or denial of service. Since sensor nodes are deployed in unattended environment an attacker can falsify local sensor values in the area of WSN and may be able to mislead monitors in those areas. So a sensor node is not able to communicate and coordinate with the network and it is disrupted. Attacks [6] against wireless sensor networks could be broadly considered from different viewpoints.

An outside attacker is a malicious node, not part of the network, but wants to harm the network, whereas an inside attacker is the one that is inside the network authorized to access the system resources but uses them in a way not approved by the granted authorization. Remote attack can be implemented from a large distance, for instance, by emitting a high-energy signal to interrupt the communication. A passive attacker just eavesdrops or monitors the packets that are transferred in a WSN. An adversary directly influences packets in the network through active attack as the fabrication of additional packages or suppression of existing packets.

In the network layer, the key issues include locating destinations and calculating the optimal path to a destination. By tampering with routing service such as modifying routing information and replicating data packets, attackers can fail the communication in WSNs. As shown in figure 1.attacks that affect the communication can be categorized into routing attack [7] and attacks on transit. In routing attack adversaries can gain access to routing paths, redirect the traffic, distribute false information to mislead routing direction or launch DOS attack against routing, acting as black holes to swallow all the received messages and selectively forwarding packets through certain sensors. The routing attacks [6] can be categorized as

- Selective Forwarding: A malicious node can selectively drop only certain packets. In sensor networks it is assumed that nodes faithfully forward received messages. But
some compromised node might refuse to forward packets, however neighbors might start using another route.

- Altered routing information: Attack against the routing information exchanged between nodes. An adversary can alter or replay routing information.

![Attacks on communication in WSN](https://example.com/attacks_diagram.png)

**Figure 1: Classification of attacks on communication in WSN**

- Sinkhole Attack: Attracting traffic to a specific node in called sinkhole attack. In this attack, the adversary’s goal is to attract nearly all the traffic from a particular area through a compromised node. Sinkhole attacks typically work by making a compromised node look attractive to surrounding nodes.
- Sybil Attacks: A single node duplicates itself and presented in the multiple locations. In a Sybil attack, a single node presents multiple identities to other nodes in the network. Authentication and encryption techniques can prevent an outsider to launch a Sybil attack on the sensor network.
- Wormholes Attacks: In the wormhole attack, an attacker records packet (orbits) at one location in the network, tunnels them to another location, and retransmits them into the network.
- HELLO flood attacks: An attacker sends or replays a routing protocol’s HELLO packets from one node to another with more energy. This attack uses HELLO packets as a weapon to convince the sensors in WSN. In this type of attack an attacker with a high radio transmission range and processing power sends HELLO packets to a number of sensor nodes that are isolated in a large area within a WSN. The sensors are thus influenced that the adversary is their neighbor. As a result, while sending the information to the base station, the victim nodes try to go through the attacker as they know that it is their neighbor and are ultimately spoofed by the attacker.

Attacks on information transit [6] can be broadly classified as interruption, interception, modification and false data injection attack.

- Interruption: is an attack on the availability of the network, for example physical capturing of the nodes, message corruption and insertion of malicious code.
- Interception: is an attack on confidentiality. The sensor network can be compromised by an adversary to gain unauthorized access to sensor node or data stored within it.
- Modification: is an attack on integrity. Modification means an unauthorized party not only accesses the data but tampers it, for example by modifying the data packets being transmitted or causing a denial of service attack such as flooding the network with false data.
3. FALSE DATA INJECTION ATTACK

Sensors are usually deployed in unattended or even hostile environments, and an adversary may capture or compromise sensor nodes. Node compromise [5] occurs when an attacker gains control of a node in the network after deployment. Once in control of that node, the attacker can alter the node to listen to information in the network, input malicious data, cause DOS, black hole, or any one of a number of attacks on the network. Once this happens, the compromised nodes can easily inject false data reports of nonexistent events. Even worse, when an adversary compromises more nodes and combines all the obtained secret keys, the adversary can freely forge the event reports which not only “happen” at the locations where the nodes are compromised, but also at arbitrary locations in the field. Table 1 shows the attacks caused by compromised nodes at different layer. These fabricated reports not only produce false alarms, but also waste valuable network resources, such as energy and bandwidth, when delivering the falsified reports to the base station. Therefore, it is important to design an effective filtering scheme [8] to defend and minimize the impacts of false data injection attack.

The four main attacks caused by the compromised node are:
- A compromised node purposely drops aggregation message
- A compromised node alters a message being relayed to the sink
- A compromised node purposely falsifies its own sensed reading
- A compromised node purposely falsifies the aggregate value it is relaying to its parent in a hierarchical network structure

<table>
<thead>
<tr>
<th>Layer</th>
<th>Attack Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical layer</td>
<td>Jamming attack</td>
</tr>
<tr>
<td>Data Link layer</td>
<td>Jamming attack, collision attack</td>
</tr>
<tr>
<td>Network Layer</td>
<td>False routing information, selective forwarding, disrupt routing protocol</td>
</tr>
<tr>
<td>Transport layer</td>
<td>False data injection, Packet dropping, Interrogation attack</td>
</tr>
</tbody>
</table>

3.1 En-route Filtering

En-route filtering is an effective way to defeat false data injection attacks. The ultimate objective of en-route filtering is to enhance the filtering capability and to improve the resilience against node compromissions. In en-route filtering that not only the destination node but also the intermediate nodes can check the authenticity of the message in order to reduce the number of hops the false message travels and thereby conserves energy. In the en-route filtering phase, every forwarding node verifies the MAC computed by its lower association node, and then removes that MAC from the received report. If the verification succeeds, it then computes and attaches a new MAC based on its pairwise key shared with its upper associated node. Finally, it forwards the report to the next node towards the BS. Figure 2 shows the general framework of an en-route filtering scheme. Here the en-route node receives a report from the source node or the lower associated en-
route node and check the integrity of the received report by means of the MAC enclosed in the report. If the verification succeeds then forward the report otherwise drop the report.

4. RELATED WORKS AND SECURITY SOLUTIONS

In WSN internal attacks are not detectable by cryptographic techniques. The unattended operation makes it easy to compromise the sensor node and to release the information to the adversary. Adversary can launch internal attack that cannot be solved by cryptographic technique [3]. Such internal attacks can be solved by en-route filtering schemes. En-route filtering schemes are useful in mitigating false data injection attack and path based DOS attack because the falsified messages will be filtered out as soon as possible.

Figure 3: Illustrate en-route filtering scheme

Figure 3 describes the general en-route filtering scheme with an example. Assume sensor nodes deployed in the area of interest is grouped into clusters. Each cluster is controlled and coordinated by a cluster head. When an event occurs in a cluster, the event information should be securely sent to base station which is assumed to be a trusted node. In the figure cluster head (CH1) generate a event report and forward the information the event report through the en-route nodes CH2, CH3, CH4 to reach the base station. The en-route nodes receive the event report verify the validity of the report through the received MAC. If found valid replace the received MAC with its MAC. Otherwise drop the report. Figure
shows en-route node CH receives a forged report found the MAC is invalid and drop the report.

4.1. Statistical en-route filtering (SEF)

Statistical en-route filtering (SEF) [9] is the first en-route filtering scheme proposed by F. Ye, H. Luo to address the fabricated report injection attacks in the presence of compromised nodes and introduce an en-route filtering framework. In SEF, there is a global key pool, which is divided into n non-overlapping partitions. Before deployment, each node stores a small number of authentication keys randomly selected from one partition of globe key pool. Nodes with keys from same partition are considered as the same group. In this way, all nodes are divided into n groups via non-overlapping key partitions. The SEF scheme adopts T-authentication, that is, the legitimate report must carry T MACs generated by T nodes from different groups. Each of these T nodes generates MAC with one of authentication keys it stored. Each event detecting sensor endorses the report by producing a keyed MAC using one of its stored keys. A report with insufficient number of MACs will not be forwarded. When the sink receives event reports, it can verify all the MACs carried in the report because it has complete knowledge of the global key pool. False reports with incorrect MACs that pass through en-route filtering will then be detected. The SEF mechanism detects and drops bogus reports from compromised nodes. The verification of MACs is done probabilistically. SEF cannot detect which nodes are compromised because reports are filtered en-route probabilistically, but it can prevent the false data injection attack with 80-90 percent probability within 10 hops. In SEF if a node is compromised the attacker can obtain the keys for number of compromised nodes since more than one node store keys from common key pool.

4.2. Secure Ticket-Based En-route Filtering (STEF)

Secure Ticket-Based En-route Filtering (STEF) [10], proposed by Krauss et al., uses a ticket concept, where tickets are issued by the sink and packets are only forwarded if they contain a valid ticket. If a packet does not contain a valid ticket, it is immediately filtered out. STEF is similar in nature to SEF and DEF. The packets contain a MAC and cluster heads share keys with their immediate source sensor nodes in their vicinity and with the sink. The drawbacks of STEF is its one way communication in the downstream for the ticket traversal to the cluster head.

4.3. An Interleaved Hop-By-Hop Authentication Scheme (IHA):

Zhu et al. proposed an interleaved hop-by-hop authentication (IHA) scheme [11]. In this scheme, the base station periodically initiates an association process enabling each node to establish pairwise keys with other nodes that are n hops away, which is a security threshold. All nodes are detecting nodes and forwarding nodes, generating reports about events, forwarding them and verifying report correctness. At least t+1 nodes must agree on a report for it to be considered valid. The drawback of IHA is, it requires the existence of a fixed path for transmitting control messages between the base station and every cluster-head. Other problem in IHA is every en-route node must exchange its associated key with lower and upper associated node. The high communication overhead incurred by the association process makes IHA unsuitable for the networks whose topologies change frequently.
4.4. Commutative cipher based en-route filtering (CCEF):
Yang et al. presented a commutative cipher based en-route filtering (CCEF) scheme [12]. In CCEF, each node is preloaded with a distinct authentication key. When a report is needed, the base station sends a session key to the cluster-head and a witness key to every forwarding node along the path from itself to the cluster-head. The report is appended with multiple MACs generated by sensing nodes and the cluster-head. When the report is delivered to the base station along the same path, each forwarding node can verify the cluster-heads MAC using the witness key. The MACs generated by sensing nodes can be verified by the base station only. CCEF has several drawbacks. First, it relies on fixed paths as IHA does. Second, it needs expensive public-key operations to implement commutative ciphers. Third, it can only filter the false reports generated by a malicious node without the session key instead of those generated by a compromised cluster-head or other sensing nodes.

4.5. Location-based resilient security (LBRS) scheme:
Yang et al. proposed a location-based resilient security (LBRS) scheme [13][14]. LBRS has a major improvement over SEF, and mitigates T-threshold limitation problem in SEF by location-ware authentication key. In LBRS, a sensing field is divided into square cells, and each cell is associated with some cell keys that are determined based on the cell’s location. Each node stores two types of cell keys. One type contains the keys bounded to their sensing cells to authenticate the reports from those cells. The other type contains the keys of some randomly chosen remote cells, which are very likely to forward their reports through the node’s residing cell. In LBRS, a forwarding node verifies the received reports and filters out false ones in the same way as SEF. LBRS suffers a severe drawback: It assumes that all the nodes can determine their locations and generate location-based keys in a short secure time slot. However, to the best of our knowledge, most of the practical sensor localization approaches [3] cannot be finished in such a short time slot, and even the localization process itself is vulnerable to various attacks. In addition LBRS cannot work effectively in the networks with mobile sink and various routing protocols.

4.6. Dynamic En-route Filtering (DEF) scheme:
In the Dynamic En-route Filtering (DEF) scheme by Yu and Guan [15][16], a legitimate report is endorsed by multiple sensing nodes using their own authentication keys. Before deployment, each node is preloaded with a seed authentication key and secret keys randomly chosen from a global key pool. Before sending reports, the cluster head disseminates the authentication keys to forwarding nodes encrypted with secret keys that will be used for endorsing. The forwarding nodes stores the keys if they can decrypt them successfully. Each forwarding node validates the authenticity of the reports and drop the false ones. Later, cluster heads send authentication keys to validate the reports. The DEF[1] scheme involves the usage of authentication keys and secret keys to disseminate the authentication keys; hence, it uses many keys and is complicated for resource-limited sensors.

VEBEK [17] is a secure network protocol for wireless sensor Network (WSN). This protocol minimize the overhead associated with refreshing keys and uses a one-time dynamic key for one message generated by the source sensor. In VEBEK uses RC4 encryption mechanism to provide simple confidentiality of the packet. The key to the
encryption is obtained from Virtual Energy based keying module. The receiving node must keep track of the energy of the sending node to decode and authenticate a packet when a forwarding node receives the packet, it checks its watch list to determine if the packet came from a node it is watching. If not the packet is forwarded without modification. VEBEK supports two operational modes VEBEK-I and VEBEK-II. In VEBEK-I mode all nodes watch their neighbors. When a packet is received from a neighbor sensor node, its authenticity and integrity are verified. VEBEK-I reduce the transmission overhead as it can catch malicious packets in the next hop itself. But increases processing overhead because of the decode/encode that occurs at each hop. In VEBEK-II operational mode, node in the network is configured to only watch some of the nodes and it cannot catch malicious packets in the next hop. In VEBEK-II more energy will be spend for node synchronization and this occurs as overhead.

4.8. A bandwidth-efficient cooperative authentication (BECAN) scheme:

BECAN[18] achieves high filtering and reliability when compared with other en-route filtering mechanisms. In BECAN each node requires fixed (k) number of neighbours for co-operative neighbor router(CNR) based authentication. BECAN filter injected false data through cooperative authentication of the event report by k neighbouring nodes of the source node. BECAN distributes the authentication of en-routing to all sensor nodes along the routing path to avoid complexity. This scheme adopts bit-compressed authentication technique to save bandwidth. The proposed technique is suitable to handle compromise and filter injected false data in wireless sensor networks. It also prevents the gangs injecting false data attack from mobile compromised sensor nodes using Ad hoc on-demand distance vector (AODV) routing protocol. BECAN is not able to address attacks such as selective dropping, false routing information injected by compromised node etc.

Analysis about en-route filtering schemes:

Many en-route filtering schemes have been proposed to reduce false data injection attack in WSN. Performance of the en-route filtering schemes can be analyzed based on false data filtering efficiency, false data filtering hops and energy consumption. The statistical en-filtering (SEF) scheme, is the first to address false data injection attack. SEF has limited filtering capacity and cannot prevent impersonating attacks. In SEF single shared key is used for generating and verifying MACs. Hence keys may be misused to generate reports. To avoid this problem, a secure ticket-based en-route filtering (STEF) Scheme was introduced with ticket concept. Here a MAC on the report uses a key shared between the en-route node and the BS.STEF produce some additional overhead due to query-response communication for the ticket traversal. But the storage requirement is very less and STEF can be used in high density network. The IHA defines a new concept of association among sensor nodes. IHA guarantees that the BS will detect any injected false data packages when no more than t nodes are compromised. In IHA there is only one path from the source cluster to the BS. This scheme requires pre-route interleaved associations maintained between sensor nodes to share the sensor secrets between upper associated nodes and lower associated nodes. Due to the unpredictable nature of the wireless medium it is not possible for a large sensor network to have determined routing paths regularly. Association among en-route nodes requires global knowledge of the network which is considered as tedious task. In CCEF the intermediate forwarding nodes are equipped with witness key which is used to verify the authenticity of the reports. But CCEF has several drawbacks. It relies on fixed paths as IHA does and it needs expensive public-key operations to implement commutative ciphers.
Table 2: Performance analysis of en-route filtering schemes

<table>
<thead>
<tr>
<th>Filtering schemes</th>
<th>Amount of authentication message</th>
<th>false data filtering hops</th>
<th>Energy efficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statistical En-Route Filtering</td>
<td>Event report contains MAC from all detecting nodes.</td>
<td>90% of false report is dropped within 20 hops</td>
<td>Saves 80% of energy</td>
</tr>
<tr>
<td>Dynamic en-route filtering</td>
<td>Event report contain authentication message from all nodes in the cluster</td>
<td>90% of false report is dropped within 10 hops</td>
<td>Saves 50% of energy</td>
</tr>
<tr>
<td>VEBEK</td>
<td>Energy value of a sending node and node id.</td>
<td>90% of false report is dropped within 15 hops</td>
<td>Saves 60-100% of energy</td>
</tr>
<tr>
<td>BECAN</td>
<td>Each report contain authentication message from all neighbouring nodes each represented with one bit</td>
<td>90% of false report is dropped within 15 hops</td>
<td>Saves 80% of energy</td>
</tr>
</tbody>
</table>

DEF has higher filtering capacity. DEF and SEF are independent of topology changes. Also it can only filter the false reports generated by a malicious node without the session key instead of those generated by a compromised cluster-head or other sensing nodes. Dynamic en-route filtering techniques are more attack resilient than static ones, a significant disadvantage is that they increase the communication overhead due to keys being refreshed or redistributed from time to time in the network. There are a lot of reasons for key refreshing which includes updating keys after revocation, refreshment of keys to avoid them from becoming old, or due to dynamic changes in the network topology LBRS suffers a severe drawback: It assumes that all the nodes can determine their locations and generate location-based keys in a short secure time slot. DEF is more complicated than SEF by introducing extra control message and the use of this control message not only increases operation complexity, but also incurs extra overhead. DEF is complicated for resource limited sensors. BECAN saves energy with reduced bandwidth. BECAN can filter false data injection attack to some extend but does not detect other attacks caused by compromised node.

Table 2: describes about the performance of en-route filtering schemes. The efficiency of the en-route filtering scheme can be detected based on the size of the message used to authenticate the event report, filtering capacity of the each en-route node on the path of data transfer, amount of energy consumed for filtering the false data injected. VEBEK consumed less energy compared to other schemes. DEF filters the false data as early as possible but the size of the authentication message required for filtering is more compared to other schemes. Table 3 specifies the case study on en-route filtering schemes.
### Table 3: Case Study on En-route Filtering Scheme

<table>
<thead>
<tr>
<th>Filtering schemes</th>
<th>Resilience</th>
<th>Network Architecture</th>
<th>Major Features</th>
<th>Overhead</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statistical En-Route Filtering</td>
<td>Information Spoofing</td>
<td>Highly dense wireless sensor network</td>
<td>*Detects and drops false reports *Event report produced by joint multiple detecting nodes.</td>
<td>It is inefficient if the number of compromised node exceeds a threshold value.</td>
</tr>
<tr>
<td>Statistical Ticket based En-Route Filtering</td>
<td>*false data injection attack. *path based DOS attack.</td>
<td>Static wireless sensor network</td>
<td>*Reports are forwarded only if they contain a valid ticket. *doesn’t require symmetric key sharing</td>
<td>Each node consumes energy to send and receive messages, to verify response messages.</td>
</tr>
<tr>
<td>Interleaved hop-by-hop authentication</td>
<td>False data injection attack.</td>
<td>Sensor nodes are organized into clusters</td>
<td>*IHA can tolerate upto ‘t’ compromised nodes. *En-route node has upper and lower association.</td>
<td>*Computation overhead due to pair wise key establishment and report authentication. *communication overhead due to T+1 MACS</td>
</tr>
<tr>
<td>Commutative cipher based en-route filtering</td>
<td>Event fabrication attacks.</td>
<td>Static wireless sensor network</td>
<td>*Defend report injection without symmetric key sharing. *Posses witness key</td>
<td>Fabricated report cannot be filtered during forwarding process.</td>
</tr>
<tr>
<td>Location based resilient security solution</td>
<td>*MAC falsification attacks. *Impersonation attacks. *Sybil attack.</td>
<td>Regular geographic grid</td>
<td>*Generate location based key. *Each node has two keys cell key and en-route key for authentication.</td>
<td>*Storage overhead each node stores one key for each sensing cell and a few remote verifiable cells. *LBRS achieves resiliency by limiting the scope for which keys are used</td>
</tr>
<tr>
<td>BECAN</td>
<td>False data injection</td>
<td>Sensor nodes deployed in certain interest region</td>
<td>*Bit-compressed authentication. *CNR based filtering mechanism. *High reliability</td>
<td>*If the source node is compromised this scheme does not function. *BECAN cannot detect false information injected by compromised node.</td>
</tr>
</tbody>
</table>
5. CONCLUSION

This paper presents the issues caused through false data injection by compromised node in WSN. In addition a review about possible attacks on communication in WSN is described. En-route Filtering is an efficient way of dealing with false data injection attacks. An analysis about the en-route filtering schemes such as SEF, STEF, IHA, CCEF, LBRS, DEF, VEBEK, BECAN has been performed. The pros and cons of the existing en-route filtering schemes are discussed. A case study is provided as a guidance to select suitable scheme according to the application on usage.

REFERENCES


AUTHORS PROFILE

S.V.Annlin Jeba: did her master’s degree in Computer Science and Engineering under Anna University Chennai, India. She is recently working as a Assistant professor in C.S.I. Institute of Technology, south India. Moreover she is a research scholar in Anna University, south India.

Dr. B. Paramasivan received M.E degree in Computer Science and Engineering under Jadavpur University, Kolkata, India. He obtained his Ph.D degree in Anna University, the area of research is Quality of Service in Wireless Sensor Networks. He is working as a Professor and Head in Department of Computer Science and Engineering, National Engineering College, Kovilpatti, Tamilnadu, India. He has published more than ten papers in International and National Journals. He has also presented more than fifteen papers in various International Conferences. He has organized more than ten seminars sponsored by various Governmental agencies. He is an active member of various professional bodies like IE and CSI.