Filtering schemes in Wireless Sensor Networks – A Survey

[1]M.Manjukavi, [2]J.Kalidass, [3]Dr.T.Purusothaman

[1]PG Scholar, [2]Assistant professor, [3]Associate Professor
Computer Science and Engineering,
Government College of Technology, Coimbatore, India

***Abstract*— Wireless sensor network(WSN) be composed of sensor nodes that are deployed densely throughout the vast province to monitor the actions such as wildfire, vehicles of the enemy on the battle field, many industrial and applications of consumer, such as industrial process control and monitoring, health monitoring, and so on. The sensor nodes are not provided with the tamper-resistant hardware because of the cost constraints, thereby increasing the chances of being compromised by the adversary through different security attacks such as selective forwarding, worm holes, node replication, node impersonate, false data injection and Sybil attacks. An adversary can compromise sensor nodes and inject fake data into the network that threaten system security and consumes network resources. To enhance the security of the network system, many filtering mechanisms have been designed. In this paper, we present the various en-route filtering schemes in wireless sensor networks.**

***Index Terms*— Wireless sensor networks, Sensor nodes, Security**

I. INTRODUCTION

Expeditious advancement in the wireless network technologies and electromechanical systems [17], the wireless sensor networks have gained growing attention due to its wide range of applications from battle field surveillance to civilian applications. For example, home automation systems, military and national defense, medical care, weather checking applications environmental monitoring, wildlife tracking, traffic management and in many other areas.

The wireless sensor network comprises of sensor nodes which are organized densely throughout vast province to monitor the events such as vehicles of enemy in the battle field, wildfire, etc. The sensor nodes are not provided with the tamper-resistant hardware due to the cost limitations, thereby increasing the chances of being compromised by the adversary through many types of security attacks, such as code injection, selective forwarding, wormholes [9] and Sybil attacks [10], node impersonation, node replication, etc.

Sensor node sense the events and create the event report for the sensed information or data and event report has to be send to the base station or server through the en-route nodes. When event report is forwarded to the server by en-route node, a compromised node can forget the report. The false data injection attack reduces the energy of the en-route nodes. One solution is to mitigate the impact of false data injection by the network through a compromised node is to filter the false injected data by the en- route node as early as possible before reaching the base station. To enhance the security of the system, many en-route filtering schemes have been developed.

II. OVERVIEW OF WSN

Wireless Sensor Networks

Wireless Sensor Networks [1] are heterogeneous systems have large number of small devices known as sensor nodes and actuators with general-purpose computing components. These networks have hundreds and thousands of low power, and self-organizing nodes, low cost, which are highly distributed which are inside the system.

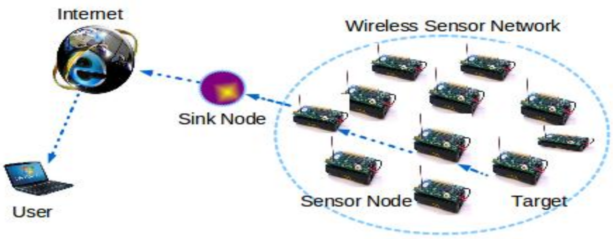

Figure 1: Wireless sensor networks

Wireless sensor networks are estimated to interact with the physical world at an unpredictable level to enable numerous applications and a large-scale sensor networks are deployed in an adverse or even in an unsafe environment which leads to the issue such as accidental failure of nodes that is false data injection. As the sensor nodes are relatively small in size and as they are deployed in the absence of human environment they are extremely sensitive to compromising of nodes is a risk. False sensing leads inject through compromised nodes, which can lead to generate the false alarms.

Security Goals

When dealing with security in WSN [2], we mainly focus on the problems, such as achieving all of the following security contributes or services:

- Confidentiality: Secrecy or Confidentiality has to do with making the data inaccessible to unauthorized users. A confidential content is resistant to illuminating its meaning to an eavesdropper.
- Availability: Availability confirms the survivability of network services to authorized parties when needed despite denial-of-service attacks. A denial-of-service attack would be launch at any of the Open System Interconnect (OSI) layer of a sensor network.
- Integrity: Integrity ensures that the received data is not changed in transit by an adversary.
- Authentication: Authentication permits a node to ensure the identity of the peer node with which it is connecting.
- Non-repudiation: Non-repudiation denotes that a node cannot late sends a message it will previously sent.
- Authorization: Authorization ensures that authorized nodes should be accessed to network services and resources.
- Freshness: This could mean key freshness and data freshness. Since all sensor networks provide some forms of time changeable measurements, we must ensure each message is fresh. Data freshness implies that each datum is recent, and it ensures that no adversary replayed old messages.

Evaluation

Besides implementing the security goal discussed above, the following metrics are also important to evaluate a security scheme should be appropriate for WSNs.

- Resiliency: Resilience is the ability of the network to provide and maintain an acceptable level of security service in case some nodes are compromised.
- Resistance: It is an ability to prevent the rival from gaining full control of the network by node replication affect in case some nodes are undermine.
- Scalability, self-organization and flexibility: In contrast to general ad hoc networks that do not put scalable in the first priority, designing sensor network must consider its scalability of its large number of sensor nodes. According to its deployment condition and changeable mission, goals, self-flexibility and organization (such as sensor networks blend, nodes joining and leaving, etc.) are also important factors when designing a secure sensor network.
- Robustness: A security scheme is robust if it continues to operate despite deviation, such as failed nodes, attacks, etc.
- Energy efficiency: A security scheme must be energy efficient so as to increases network lifetime.
- Assurance: It is an ability to disperse distinct information at different assurance levels to the end-user. A security scheme [5] had better allow a sensor network to deliver different level information with consider to different desired latency, reliability, etc. with different cost.

Security Challenges

The security challenges in sensor networks [4] from as follows:

- Minimizing resource consumption and maximizing security performance.
- Sensor network distribution renders more number of link attacks ranging from passive eavesdropping to active interfering.
- In-network processing associate intermediate nodes in an end to end information transfer.
- Wireless communication characteristics render classic wired-based security schemes unfit.
- Large scale and node moveable make the affair more complicated.
- Node count and downfall make the network topology dynamic.

Applications of wireless sensor networks

False sensing reports can inject through adjust nodes, which should lead to improper alarms. Wireless sensor networks have gained considerable popularity because of their flexibility in solving problems in various application domains [8] and have the potential to change our lives in many different ways.

Military applications: Wireless sensor networks are likely an integral part of control, military command, computing, communications, battlefield surveillance, intelligence, targeting systems and reconnaissance.

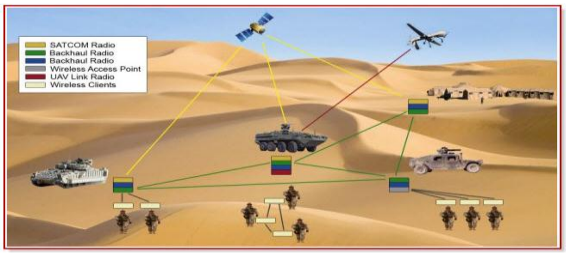

Figure 2: Military application

Area monitoring: In area monitoring, the sensor nodes are deployed over a region where some aspect is to be supervise. When the sensors detected the event being monitored (heat, pressure, etc.), the event should be reported to one of the base stations, which then takes relevant action.

Transportation: Real-time traffic information is being collected by WSNs to ensuing feed transportation models and alert drivers of congestion and traffic complication.

Health applications: A few of the health applications for sensor networks are supporting interfaces for the infirm, combined diagnostics, patient monitoring, tele-monitoring of human physiological data and narcotic administration in hospitals, and trace & monitoring doctors or patients inside a hospital.

Environmental sensing: The term Environmental Sensor Networks have developed to cover many applications of WSNs to earth science research. This includes sensing glaciers, forests, volcanoes, oceans etc. Some other major areas are listed below:

- ➢ Air pollution audit
- ➢ Forest fires strike
- ➢ Greenhouse observer
- ➢ Landslide disclosure

Structural monitoring: Wireless sensors can be utilized to monitor the development within buildings and infrastructure such as tunnels, embankments, flyovers, bridges, etc. Permissive Engineering practices to monitor assets remotely without the need for pricey site visits.

Industrial monitoring: Wireless sensor networks should be developed for machinery condition-based maintenance (CBM) as they offer compelling enable new functionalities and cost savings. In wired systems, the installation of acceptable sensors is generally limited by the cost of system.

Agricultural sector: Using a wireless network frees the farmer from the maintenance of system in a crucial environment. Irrigation computerization enables more efficient water use and reduces waste.

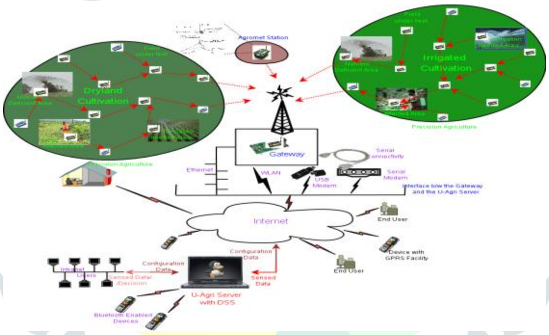

Figure 3: Agriculture application

Routing Attacks in Sensor Networks

Wireless Sensor networks are vulnerable to security violation due to the newscast nature of the transmission phase. Furthermore, wireless sensor networks have an additional burden because nodes are often placed in a dangerous or hostile environment where they are not physically secured. The attacks which is on the network layer are known as routing attacks. The following are the attacks [3] that happen while routing the messages.

Wormhole: Wormhole attack [9] is a severe attack in which two mugger placed themselves strategically in the network. The muggers then keep on hearing the network, record the wireless data. In a wormhole attack, an attacker gets packets at one point in the network, "channel" them to another point in the network, and then replays them into the network from that point.

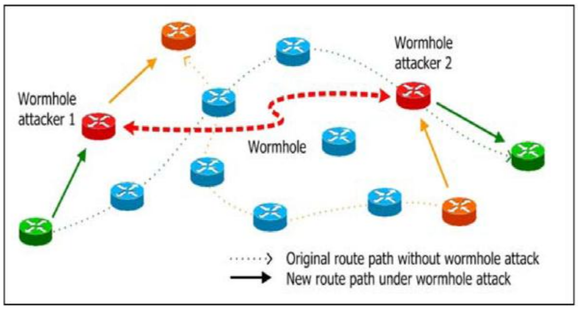
Wormhole attacker 1
Wormhole attacker 2
Wormhole
Original route path without wormhole attack
New route path under wormhole attack

Figure 4: Wormhole attack

An attacker intrudes communications originated by the sender, copy a section or a whole packet, and speeds up sending the copied packet through a specific wormhole tunnel in such a way those are copied packet arrives at the destination before the pioneer packet which pass over through the expected routes. In such a tunnel should be created by multiple means, such as by sending the copied packet via a wired network and at the edge of the tunnel transmitting up a wireless channel, using a assist long-distance antenna, sending over using any out-of bound channel, or a low- latency route. The wormhole attack poses many threats, especially to routing protocols and some other protocols that are heavily await on geographic location and proximity, and many subsequent attacks [18] (e.g., selectively forwarding, sinkhole) can be launched after the wormhole path has attracted a large amount of traversing packets.

Impersonation: In wireless networks a node is free to move in and out of the network. There is no security authentication process in order to make the network secure from malicious nodes. The attacker uses MAC and IP spoofing in order to get identity of another node and hide into the network. This kind of attack is also known as spoofing attack. Impersonation attacks are launched by using other node's identity, such as MAC or IP address. Feigning attacks are the first step for major attacks, and are used to pitch further more experienced attacks. An attacker impersonates another node's identity (either MAC or IP address) to establish a connection with or drive other attacks on a sufferer; the raider may also use the victim's identity to establish a connection with launch other attacks or other nodes on favor of the victim. An attacker illegitimately uses the victim's credentials to approach the Server. There are many software's capable of reprogramming the devices to forge the MAC and network addresses.

Selective Forwarding: Selective forwarding attack is one of the harmful attacks against sensor networks and should be affect the entire sensor network communication. In such attacks, malicious nodes may refuse to forward certain packets and simply drop them, ensuring that they do not propagated any further. An adversary will not, however, drop all packet. To eliminate raising suspicions, the attacker instead selectively drops packets originating from a few selected nodes and forwards the remaining Traffic. This attack is sometimes called Gray Hole attack. In a simple form of selective promote attack, malevolent nodes crack to stop the packets in the network by refusing to forward or drop the messages passing along them. There are many forms of selective forwarding attack. In one form of the selective forwarding attack, the malicious node can selectively drop the packets coming from a particular node or a group of nodes. This act causes a DOS attack for that selective node or a group of nodes. A forwarding node selectively drops packets that are forwarded or originated by some nodes, and forwards other irrelevant packets instead. They also works like a Black hole in which it restricts to forward all the packet. The malicious node may forward the packets to the wrong path, producing untrue routing information in the network. A malicious node can selectively drop only particular packets. Especially active if joined with an attack that gathers much traffic via the node. In sensor networks, it is pretended that nodes faithfully forward got messages. But some compromised node might not accepted to forward packets, however nearby roots might start using another route.

Spoofing: Spoofing attack [6] is a situation in which one human or computer program successfully carnival as another by falsifying data and thereby gaining an illegitimate advantage. Spoofed, altered and replayed routing information

- An un secured ad hoc routing is dangerous to this types of attacks, as every node acts as a router, and can therefore straightly affect routing information.
- Create routing loops
- Extend or shorten service routes
- Generate false error messages
- Increase end-to-end latency

Node replication attack: It is an attempt by the adversary to improve one or more nodes to the network that use the exactly same ID as another node in the network. The node replication attack or the clone node attack should a security hazard where an attacker creates its sensor nodes and joins the network as if they are the appropriate nodes of the network. For this attack to happen, the attacker will physically abduction one node from the network and excerpt all the secret information of the node such as node ID, Keys etc. The replication attack can be awfully adverse to many important functions of the sensor network such as resource allocation, routing, misbehavior detection, etc.

Sybil attack: A single node presents itself to other nodes with multiple spoofed identifications (either network addresses or MAC). The attacker should imitate other node identities or simply create multiple inconsistent identities in the MAC and/or network layer. The attack poses threats to the other protocol layers; for examples, packets traversed on a route consisting of fake identities are selectively discarded or modified; or a threshold-based signature mechanism that relies on a specified number of nodes is perverted. A single node duplicates itself and presented in the multiple locations. The Sybil attack [10] targets fault tolerant schemes such as distributed storage, multi-path routing and topology conservation. In a Sybil attack, node presents multiple identities to other nodes in the network. Authentication and encryption techniques can preserve an outsider to launch a Sybil attack in the sensor network.

Sinkhole Attack: Attracting traffic to a specific node in called sinkhole attack. In this attack, the adversary's ambition is to bring nearly all the traffic from a particular area through a compromised node. Sinkhole attacks typically work by making a compromised node look exclusively enticing to surrounding nodes.

HELLO flood attacks: An attacker sends or replays a routing protocol's HELLO packet from one node to another with more energy. This attack uses HELLO packets as a weapon to convince the sensors in WSN.

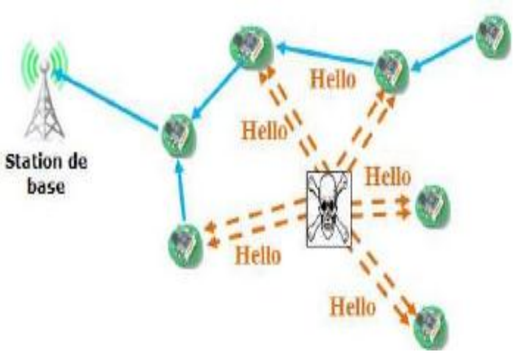

Figure 5: Hello flood attack

In this type of attack, an attacker with a high radio transmission length and processing power sends HELLO packets to a number of sensor nodes that are detached in a large area within a WSN. The sensors are thus altered that the competitor is their neighbor. As a result, while sending the information to the base station, the fatality nodes try to go through the attacker as they know that it is their neighbor and are basically mislead by the attacker.

Node compromise: A new challenge in the wireless sensor networks (WSN) is the negotiate nodes problem. Negotiated node [7] may exhibit erratic behavior and may connive with other compromised nodes. A compromise node involves the addition of a node by an adversary and causes the injection of malicious data. An criminal might add a node to the system that feeds false data or prevents the flows through of true data. Insertion of malicious node is one of the most dangerous attacks that can occur. Malicious code injected into the network could spread to all nodes, possibly spoiling the whole network, or even bad, taking over the network on behalf of an adversary.

Wireless Sensor Network (WSN) is often deployed in hostile environments as static or mobile, where an adversary should physically capture selection of the nodes. Once a node is captured, adversary collects all the accreditation like keys and identity, etc. To reduce the routing attacks and complement the security of the system, many en-route drain schemes are developed.

Compromised nodes can do the following attacks:

• Compromised node can steal secrets from the encrypted data which was passed it;
• Compromised node can address wrong information to the network;
• Compromised node can report some of the normal nodes as compromised nodes;
• Compromised node can breach routing by introducing many routing attacks, such as black hole, selective forwarding, changed the routing data, etc., while systems are hard to attention these activities, and orderly encryption methods have no effect to anticipate them because they own the secret information such as keys;
• It may exhibit arbitrary behavior and may collude with other compromised nodes.

III. LITERATURE SURVEY

Statistical En-route Filtering (SEF)

It is the most basic mechanism in which dense deployment of large sensor networks carried. To avoid any single compromised node from breaking down the entire system, SEF [11] sends only limited by the amount of security information assigned to each node and depends on the collective decisions of multiple sensors for faulty report detection. As a report is forwarded concluded multiple hops toward the sink, each intermediate node verifies the exactness of the MACs carried in the report and crumb the report if an incorrect MAC is detected. In SEF large count of sensor nodes are extent densely. Each of the sensing nodes causes a keyed MAC (Message Authentication Code). It is assumed that multiple sensor nodes can detect the same event, so each detected event is assigned with multiple MACs. SEF limits the quantity of the classified information to be accredit to each node to protect the network break down through a single compromised node and relying on the mutual decision made by the neighboring nodes that have detected the same event. Each of the sensing node deliver the discern signal density and one of the sensor node is chosen as the Centre-of-stimulus (CoS) node. The CoS then composes and encapsulates the detecting event and make a combined report. The report is forwarded to the sink node by passing through the large number of hops. Each sensing node in the en-route verifies the correctness of the report by sensibility the MACs with pre-defined probability and dismiss the report with invalid MAC. With the increasing number of bound, the probability of disclose invalid MACs also improves. Some of the reports may departure from the en-route filtering and reach the destination. The destination node (sink) further verifies the correctness of the MAC and drops the false reports.

SEF has the following aims:

(i) Firstly Detection of false data reports: Detecting and dropping the false reports originally can save the bandwidth and energy of the network.

(ii) Low computation and communication overhead: Taking the resource constraints of the sensor nodes into consideration, the asymmetric cryptography has been eliminated and its efficient one-way hash function should be used. It limits the number of confidential information to be assigned to every node. The more the security information gives in the node, the more successful transit sifting can be used. For the privacy of the event, certain amount of confidential information should be given to a node, the adversary can access the safer information by compromising only by one of the node. Thus to overcome this problem, SEF divides its global key pool into barrier and each barrier is assigned a certain number of keys.

The disadvantage of SEF is the probability of distinguish faulty MACs increases with the number of hops the report travels. SEF has the T-threshold condition. That is, if the adversary compromises T nodes from different groups, they could inject false data to generate the false report.

Interleaved Hop-by-Hop Authentication (IHA)

Zhu et al. presented an interleaved hop-by-hop authentication (IHA) scheme [12] for filtering of injected false data. In IHA, each node is associated with two other nodes along the path, Lower association node and Upper association node. An en-routing node can forward the received report if it is profitably verified by its lower league node. To reduce the size of the report, the scheme compresses individual MACs. The security of the scheme is mainly unforeseen upon the creation of associations in the association discovery layer. Once the formation fails, the security cannot be approved. The symmetric keys from a key pool which allows the compromised nodes to misuse these keys to generate false reports. The IHA scheme focuses on detecting and filtering the false data at en-route nodes or sink or at the base station. This scheme is widely used in large-scale wireless sensor network, where the sensed data need to be sent via many hops before reaching to the base station. In IHA scheme, the sensor nodes are organize into clusters with a unique cluster ID. Each cluster comprises of t+1 sensor nodes, where the pretend threshold and one of the node is selected as the cluster head. This scheme assures that the base station distinguish the false data implant by the adversary, if there are less than t compromised nodes. Given a threshold t, and upper bound B is gives, for the number of hops, the report to be through before it is founded and rejected. The network is two way, that is, if node a can communicate with node b, then node b can also connect with node a. And all node in the network should share its master key with the base station. Each node coordinate its one-hop near able node and has to establish the pair wise key. Each node has two association nodes, one is lower association node and other upper association node. The report is delivered ahead only if it is verified by the lower association node.
This scheme has the following properties:
(i) If a false data has been append by the compromised nodes, then the base station is qualified enough to detect them.
(ii) The number of hops that a false data is to be detected and expelled should be smaller.
(iii) Then mechanism is efficient in computation and communication regarding the security.
(iv) The scheme should be tough towards the node failure.

The IHA needs the fixed route to transmit messages between the base station and the cluster head. Theses, creating it inadequate for the network topologies that frequently changes. Moreover, if the cooperative fails, then security cannot be approved.

Location-based Resilient Security (LBRS)

Yang et al [13] proposed Location-Based Resilient Security (LBRS), which adopts location key binding mechanism to reduce the damage made by node compromise, and further mitigate the false data creation in wireless sensor networks. To achieve en-routing filtering, evidence aloft are required additional 20 bytes. The LBRS scheme overcomes the problem of threshold that were encountered in previous schemes. This is the location based mechanism in which the secret keys are confined to the geographic location and few keys are stored within its own location. This location-binding technique limits the breadth of the key misuse. In this scheme, the terrain is disband into square cells and each of these cells is provided with some cell keys based on its location. Each node in the cell contains two types of keys, one to authenticate the report within the cell and other keys are anyway chosen for remote cells. This scheme uses two techniques: one is location-binding keys and the other is location-based key position.
It has high flexibility to the number of compromised nodes for the following reasons:
(i) It averts the attacker from arbitrarily corruption a compromised key, because the keys are limited to its geographic location and can be used only with its location.
(ii) Limits damage if the adversary compromises many nodes and acquire the keys, because group of keys are appoint to a different location and cannot be used together.
(iii) At the end, limits the number of keys to be stored into the node as each node is hire only a few keys depending upon its location.
This scheme has a severe flaw, it is affected that individual node can determine its location and can cause location-based keys in a short time slot. But this task cannot be finished in such a short time slot. And the process of localization itself is ready to various attacks. This scheme does not provide end-to-end data security.

Location-aware End-to-End Security (LEDS)

The filtering schemes provide hop-by-hop security and do not ensure end-to-end data security. To overcome this problem Ren et al. proposed [14] more efficient location-aware end-to-end data security design (LEDS) to provide end-to-end security guarantee counting efficient en-routing, false data filtering capability and high-level assurance on data availability. To achieve en-routing filtering, additionally 20 bytes authentication overheads are required. It assumes that all the nodes can determine their locations and generate location- based keys in a short secure time slot. LEDS scheme that provides end-to-end data security and taking the advantage of the broadcast nature of the sensor network, LEDS also provides one-to-many data delivery approach. This scheme exploits static and location-aware security paradigm in sensor network. It consists of two techniques: a location- aware key management framework, and an end-to-end data security mechanism.

1. **Location-aware key management framework**: Management of keys in LEDS depends on the static and location- aware nature of sensor nodes. A robust and efficient location-aware key management is achieved by lodging the location information into the keys. In LEDS, each node has three types of keys: (1) Two unique secret keys, shared between the sensor nodes and the sink. (2) A cell key, shared among the sensor nodes within the cell. (3) A set of authentication keys, shared with report - authentication cells

that provide authentication between cells and filter false data. All these keys are computed by each individual node independently and locally.

2. **End-to-End data security mechanism**: It ensures data confidentiality by encrypting the report with the cell key of the corresponding cell. Since, the cell key is shared among all the sensor nodes within that cell and with the sink, data confidentiality is ensured until no node in the cell is compromised. It also ensured data availability by providing a strong shield against report demote and selective forwarding attacks.
LEDS has following features:
(i) The targeted area is virtually divided into a number of cells using a virtual geographic grid. Then the location information is provided with each key owned by a node.
(ii) Guarantees end-to-end data security, by encrypting unique key with each report. Furthermore, the authenticity of data can be individually verified by the sink.
(iii) Have efficient en-route filtering mechanism to filter the false data injected by compromised nodes.
(iv) Finally it assures high level data availability by counteracting both report disruption and selective forwarding attacks simultaneously. Like LBRS, LEDS also assumes that sensor nodes can determine their location and generate their own location based keys in a short time slot, which is not possible. LEDS addresses selective forwarding attacks, by allowing all the nodes within the cell to forward the reports, which results in communication overhead. This scheme also has t-threshold limitations, if the number of compromised nodes are more than t, then security cannot be guaranteed.

Group-based Resilient Statistical En-route Filtering Scheme (GRSEF)

Yu et al. proposed GRSEF scheme [15] that tries to overcome the problems of SEF mechanism. In GRSEF, the nodes are divided into t-groups after the sensor nodes are deployed. Thus, increase the probability of covering any position by different groups. Before deployment, every node is provided with a global master key, which is used to compute the group master key. The group master key is then integrated with the multiple axes-based methods to compute authentication keys. The GRSEF does not depend on the sink. It improves the filtering efficiency by dividing the sensor nodes into a certain number of groups and assigns authentications to the groups. GRSEF employs a multi-axis division technique to overcome the threshold limitation problem that we have seen in the SEF and IHA. When an event occurs, the nodes detect the event and generate a MAC using authentication keys. It then sends the group number and encrypted MAC to the cluster head. The cluster head is responsible for collecting all the group numbers and MACs from the neighboring nodes and then make a combined report and send it to the base station. Each node in the path that receives the report uses the event location to verify the MAC by deriving the partition-binding keys. If a node in the forwarding path receives invalid MAC or the number of MACs is less than the predefined threshold T, then the report is discarded. When the report is received by the base station, it derives all the keys by global master key and verifies the MAC in the report. However, GRSEF has some drawbacks; it does not provide resilience to selective forwarding attack and report disruption. It has threshold limitations. It is not suitable for the topologies that changes frequently. Computing and maintaining multiple axes-based keys increases communication and cost overhead.

TABLE I. PROS AND CONS OF EXISTING FILTERING SCHEMES

Scheme	pros	cons
SEF	• Grouping-based shared key mechanism, • Reduce the communication overhead, • Independent of data dissemination protocol.	• *T*-threshold problem, • No resilience to the selective forwarding attack and report disruption attack
IHA	• First deterministic en-route filtering scheme, • Utilizing node association, • Adopting an interleaved hop by-hop authentication approach	• *T*-threshold limitation, • Relies on specific data dissemination, • High communication overhead
LBRS	• Utilizes the location-binding key generation and location-guided key selection techniques	• Relies on special data dissemination protocol, • Requires node localization

LEDS	- Utilizes the location-ware key, - High resilience	- High communication Overhead, - Relies on specific data dissemination route, - Requires node localization and takes a long time to be stable
GRSEF	- Utilizes a multi-axis division technique,	- Does not apply to the networks with dynamic topology, - Has no resilience to the selective forwarding attack and report disruption attack.

Polynomial-based Compromise Resilient En-route Filtering (PCREF)

In Cyber Physical Networked System, the sensor nodes monitor the physical component and obtain measurement, process those measurements and then the measured data is forwarded to the controller. The controller after receiving the measurement reckons the state of the system and transmits the commands to the actuator to handle the system's operation. The wireless sensor networks are used to estimate the state of the CPNS. The sensor nodes in the CPNS lack in tamper resistant hardware and thus are prone to various attacks like node impersonating attacks, node replication attacks and false data injection attack is one of the attack that thwart the security of the system. Hence, the false data must be detected and dropped before it reaches the controller and making the controller to estimate the wrong physical state of the system.

The schemes that are discussed in literature survey have some limitations and thus are not suitable for CPNS. Therefore, Yang et al. proposed Polynomial-based Compromise Resilient En-route Filtering (PCREF) scheme [16] that uses polynomial for the report authentication instead of using MACs that ensure high resilience to the number of compromised nodes without depending on the static data routed and node localization and achieve a high filtering probability of false injected data. PCREF scheme consists of two types of sensor nodes, one is sensing node and another is forwarding node. The sensing nodes are responsible for sensing the measurement, endorse and forward the report of sense measurement along the path. Forwarding node is used to just forward the received reports towards the controller. Each node in the network stores, two types of polynomials; Authentication polynomial and Check polynomial. Sensing node contains the authentication polynomial of the local cluster and check polynomial of the remote cluster with some predefined probability. The forwarding node stores only the check polynomial with same probability of each cluster. The polynomials are tied with the node ID and the polynomials are derived from the primitive polynomial pool. This scheme is independent of the static route because, the statistical pre assignment is used to share the authentication data instead of using node association.

Besides, the PCREF uses cluster-based polynomial assignment to compute the authentication and check polynomial, thus each cluster is assigned different polynomials. So that, if some nodes are compromised in a cluster, those cannot affect the security of another cluster, thus it limits the effect of attack nodes within a particular cluster. PCREF scheme has two key components: (i) authentication information assignment that is used to assign the keys, authentication polynomials, check polynomials and sensing nodes local ID and (ii) data security management, that is used for the detection and filtering of false measurement reports.
These components are discussed briefly in the following subsections.

Authentication Information Management: In this phase, a master key and a global polynomial pool need to be prepared before the sensor nodes are deployed. The master key is generated and stored in the sensor node before deployment, which is further used for computing the cluster key for each cluster in the network. The polynomial pool consists of various ternary polynomials that are created randomly before sensor node deployment. There is a hash function H (.), whose domain is encrypted measurement by sensing nodes and range is the set of positive integers.

This phase has four steps.
Cluster Organization: Sensing nodes are organized into clusters and they monitor the physical component. The sensing nodes can be deployed in a place close to the component. A node communicates with each other and stores the node Ids of only other n-1 nodes within a cluster. A node cannot store the node ID of other cluster even if it is only one hop away.

Authentication information assignment: In this phase, the network and all other nodes are initialized with the parameter {KC , f (x, y, z), T, H (.)}, where K C is the master key, f (x, y, z) is the set of polynomial with parameters x representing all the sensing node Ids, y representing all forwarding node Ids, and z representing all the measurement reports. T is the threshold and H(.) is the hash function. Then using these parameters the designer computes the authentication polynomial and check polynomial.

Key generation: In this phase, the sensing uses the master key and generates the cluster key. The master key and the cluster head ID are concatenated and a new string is generated that is used as the cluster key. The master key is erased after the network deployment.

Local ID assignment: Cluster head assigns a local ID to each sensing node. This phase is carried out after the sensor network deployment.

Data Security Management: This phase is concerned with the detection and filtering of the false measurement reports. This is carried out by following four steps.

Sensing report generation: The sensing node monitors the physical component, measures the data and creates a measurement report r. This report consists of the encrypted measured data, local ID, node ID and Message Authentication Polynomial (MAP). For the same measurement report, sensing node generates various MAPs using node ID and authentication polynomial. Once the sensing node generates the report, it is then forwarded to the cluster head.

Measurement report generation and transmission: Once the cluster head receives all the measurement reports r generated by the sensing node, it then randomly selects T reports among them and combines the selected reports to an integrated measurement report r and then the cluster heads forward this report R to the controller along the route.

En-route filtering: The en-route filtering is done with the false reports injected by the compromised nodes. The measurement report is transmitted hop-by-hop to the controller. The intermediate node that is having the check polynomial verifies the correctness of the received measurement report.

Controller authentication: After the measurement report is received by the controller, the controller authenticates the report in the same way as the intermediate node does. As the controller has all the polynomials, cluster keys and master key, it can verify all the measurement reports and filter out the false reports.

IV. Conclusion

In order to detect the false data injection attacks, many filtering schemes have been proposed. But most of them either have T-threshold limitation or rely on static routes and node localization. Hence, PCREF scheme has been proposed by yang et al. which can filter false data effectively and have resilience to the compromised nodes without depending on static routes and node localization. PCREF uses polynomials instead of MACs for verifying the reports and uses cluster based polynomial assignment. Yang et al. concluded that this scheme has better filtering capability and high resilience to the compromised nodes as compared with existing schemes.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: A survey. Computer Networks, 38(4):393–422, 2002.

[2] Adrian Perrig, John Stankovic, David Wagner, "Security in Wireless Sensor Networks" Communications of the ACM, Page53-57, year 2004.

[3] Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", AdHoc Networks (elsevier), Page: 299-302, year 2003.

[4] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009.

[5] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks, " IEEE Commun. Surveys Tutorials, vol. 8, pp. 2–23, year 2006.

[6] H. Chan and A. Perrig, "Security and privacy in sensor networks," Computer, vol. 36, no. 10, pp. 103–105, 2003.

[7] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Node compromise modeling and its applications in sensor networks," in Proc. IEEE Symposium Computers Communications (ISCC), 2007.

[8] S.Prasanna, Srinivasa Rao, "An Overview of Wireless Sensor Networks Applications and Security"in proc of International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-2, May 2012.

[9] Zaw Tun and Aung Htein Maw,(2008)," Worm hole Attack Detection in Wireless Sensor networks", proceedings of world Academy of Science, Engineering and Technology Volume 36, December 2008, ISSN 2070-3740.

[10] J.R. Douceur. "The Sybil Attack". Proc. 1st ACM Int'l. Wksp. Peer-to-Peer Systems, 2002.

[11] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route filtering of injection false data in sensor networks," IEEE J. Sel. Areas Commun., vol. 23, no. 4, pp. 839–850, Apr. 2005.

[12] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-by-hop authentication scheme for filtering of injection false data in sensor networks," ACM Trans. Sensor Netw., vol. 3, no. 4, pp. 259–271, 2007.

[13] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, "Toward resilient security in wireless sensor networks," in Proc. 6th ACM Int. Symp. Mobile Ad Hoc Netw. Comput. (MobiHoc'05), 2005, pp. 34–45.

[14] K. Ren, W. Lou, and Y. Zhang, "Leds: Providing location-aware end to end data security in wireless sensor networks," IEEE Trans. Mobile Comput., vol. 7, no. 5, pp. 585–598, May 2008.

[15] L. Yu and J. Li, "Grouping-based resilient statistical en-route filtering for sensor networks," in Proc. 28th IEEE Int. Conf. Comput. Commun. (INFOCOM), 2009, pp. 1782–1790.

[16] Xinyu Yang, Jie Lin, Wei Yu, Paul-Marie Moulema, Xinwen Fu, and Wei Zhao, " A Novel En-Route Filtering Scheme Against False Data Injection Attacks in Cyber-Physical Networked Systems", IEEE Trans on Computers, vol.64, no.1, January 2015.

[17] Wang, Ding, and Ping Wang. "On the anonymity of two-factor authentication schemes for wireless sensor networks: Attacks, principle and solutions." Computer Networks 73 (2014): 41-57.

[18] J. Lin, X. Yang, W. Yu, and X. Fu, “Towards effective en-route filtering against injected false data in wireless sensor networks,” in Proc. IEEE Global Telecommun. Conf. (GLOBECOM), 2011, pp. 1–6.

[19] M. Anand, E. Cronin, M. Sherr, M. Blaze, Z. Ives, and I. Lee, “Sensor Network Security: More Interesting Than You Think”, In Proc. of the 1st USENIX HotSec, 2006.