A Novel En-route Filtering Scheme against False Data Injection Attacks in Cyber-Physical Networked Systems

Kiran B. Giri, Rajendra S. Kanphade, Bhagyashri Warhade
Department of Electronics and Tele Communication Engineering,
Nutan Maharashtra Institute of Engineering and Technology, Talegaon Dabhade,
Savitribai Phule Pune University, India

ABSTRACT

In last decade, applications of wireless sensor systems (WSNs) i.e. Cyber-Physical Networked Systems (CPNS), have been expanded because of its tremendous potency to interface the physical world to the practical world. In CPNS, third party like attackers could insert wrong estimations to the controller by trading off a sensor nodes in networked system, which not just in danger the security of the system, additionally utilizes system resources. To determine such issue, various en-course filtering has been intended for wireless sensor networks.

So the proposed system is a Polynomial-based Compromised-Resilient En-course Filtering plan, in this proficiently filters false data efficaciously as well as accomplish an eminent quality strength to the numeral of traded off nodes without trusting upon stable route and node lateralization. To accomplish the versatility of attackers the scheme user's polynomials rather than message authentication codes (MAC) for underwriting measurement results. All node stores two kinds of polynomials: authentication (hallmark) polynomial (multinomial) and check polynomial got from the primitive polynomial, and used for underwriting as well as checking estimated results.

Keywords

Cyber-physical networked system, false measurement report, polynomial-based en-course filtering.

1. INTRODUCTION

In any case, because of the utilization of big numbers of sensor nodes in WSN [1], detection of failed or malfunctioning sensor node is essential. It has affected the reliability and efficiency of WSN. To achieve and maintain the high quality of WSN, detection of miss functioning sensor node is essential.

WSN are requisite to interface with the practical world at an uncommon level to authorize different new usage. Because of the little sizes and unattended actions, sensor nodes have a high endangerment of being acquired. False detecting results (documents) will be inserting in the network through traded off nodes, which can prompt false alerts as well as the exhaustion of restricted energy assistance in a battery fueled system [2].

The false information infusion in a CPNS is achieved by using the creation of clump also called cluster where the neighbor sensor node with same function will be organized in the form of clump. In the various leveled system structure every cluster has a pioneer which is known as cluster head (CH). The sensor nodes sporadically convey their data towards the CH nodes. CH adds up the data and conveys that results to the base station (sink) either directly or through the medium communication with other Cluster Head nodes [3].

The data received from all the sensor nodes, the BS is the information processing unit for that receiving data. The place of base station is fixed. The mapping of each Cluster Head is to perform basic functions for every one of the sensor nodes in the entire cluster, such as gathering the information earlier diverting it towards the sink. Somehow, the CH is the base station for all the cluster nodes [4].

The benefit of cluster based circumstance are:

1) Encouraging network measurability as well as diminishing energy utilization through information collection

2) It can restrict the path style inside the cluster and in this way decrease the length of the routing table stored at the common node. The principle parameters incorporated into cluster are: Number of groups/clusters, Nodes and Cluster Heads versatility, Nodes case and function, Cluster organization methodology, CH choice.

2. RELATED WORK

In past number of strategy have been described for filter out false information in WSN where the data is transferred in surroundings where the sensor nodes are strewing. For example in Statistical En-course Filtering Scheme, Interleaved Hop-by-Hop Schemes have the restriction of node compromising where the false information can be injected to developed the false reports [4].

The compromise resilient en-course filtering scheme where the sensor nodes are manage in the cluster form. And the data is conveyed to Base station (sink) by using forwarding nodes which act as an intermediate between the cluster and the base station (sink).

Statistical en-route filtering is the en-course filtering technique to reference the constructed report infusion attacks in the inherence of compromised nodes and present an en-course filtering model [5]. In SEF, there is a worldwide central pool, which is isolated into n non-covering segments. Before arrangement, every node stores a little number of validation keys arbitrarily chose from one parcel of globe key pool [6]. Once a input appears in the network field, various nodes choose a center of stimulus (CoS) hub that creates the results. Every detecting sensor delivers a MAC for the report utilizing one of its put away keys. The CoS hub gathers the MACs and then joins both to the report as a Bloom filter. The number of MACs comically acts as the confirmation that a report is logical. The BS verifies every MAC because it knows all the MACs keys when base station receives reports. If incorrect information with wrong MACs that furtive through en-course filtering unfortunately are still detected [4].

Secure Ticket-Based En-route Filtering (STEF), 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 nature to SEF and DEF[4]. 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 are its one way communication in the downstream for the ticket traversal to the cluster head.

In Commutative Cipher Based En-course Filtering, each node is loaded with the particular confirmation key. At the point. The BS forwards a session key to the head and a witness key to every sending hub when a result is required [8]. The report is attached with number of MACs generated by sensing nodes and the cluster-head. When the result is convey towards the sink with the same way, every forwarding node can check the cluster-heads MAC with the help of witness key. The MACs produced by detecting hubs can be confirmed by the BS. CCEF has a few disadvantages. It needs costly open key commission to enforce commutative ciphers [8].

PCREF utilizes polynomials rather than MACs to check result and can moderate the node portray attack against logical nodes. By arranging the sensing nodes in a the form of cluster, PCREF designate the authentication polynomial and check polynomial to every sensor nodes in the network [7]. These polynomials are issued in a nodes are bundled with node. Dissimilar primitive polynomials will be used in every cluster through the cluster-based primitive polynomial scheme. This cluster based environment increases the strength of our plan to the expanding number of traded off hubs without depending on the hub limitation and static information spread courses. To support the result of general element activity the authentication polynomial issued in every node and the check polynomial is used to formalize the standard results

3. BACKGROUND

Presenting a methodology called Polynomial-based Compromised-Resilient En-course Filtering plan for Cyber-Physical Networked Systems, this schemes filter false infused data viably and accomplish a high rebound to the number of endanger nodes which doesn't relies on upon the stable data circularize path and node determination. PCREF clinches polynomials instead of MACs to check reports, and can alleviate node representing attacks against logical nodes. In this approach, distribute the authentication content or message between sensing nodes with the earlier defined probability avert the node related to contribute authentication message or data between initial nodes and forwarding nodes, therefore this approach can’t operate upon stable path.

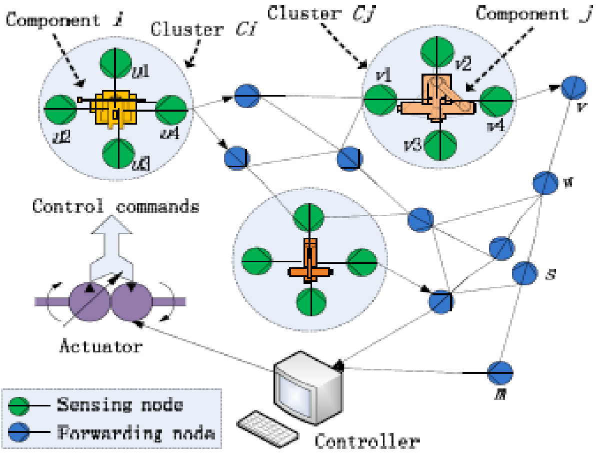

Fig 1: System Architecture

There are two types of nodes in the system, sensing nods and forwarding nodes, shown as green nodes and red nodes in fig. These two types of nodes are denoted as sensor node and forwarding nodes in this paper. The two nodes in fig connected with bidirectional link means that these two nodes are within each other’s wireless communication range and communicate with each other directly. The sensing nodes can not only sense and form the measurement reports of the monitored components, but also forward the measurement reports of other nodes. The forwarding nodes can only forward the measurement reports to the controller. We assume that each cluster has a unique id and each node has a unique node id.

4. EN-ROUTE FILTERING

The en route filtering is technique used in wireless networks with which the intermediate nodes checks the correctness of the data that is being travelled along the route from source to the sink with the help of intermediate nodes present in the network. The intermediate node not only checks the correctness of the data but also can filter the false data effectively. The intermediate nodes after receiving the report checks whether it contain valid T-MAC. The report with less number of T-MAC will be dropped. If any false data which is not filtered by the intermediate nodes will be detected by the sink where it gets filtered. The sink acts as the final defense that catches false reports not filtered out by forwarding nodes.

4.1 Modules

This scheme consists of the following modules key components:

1) Authentication and information management
2) Data security management

4.1.1 Authentication and information management

In this module they assign the key, authentication polynomial, check polynomial, and local ID of sensing nodes. At first they assume that the node initialization phase is reliable and secure, and the attacker cannot compromise and launch attacks at any node during this phase. The node initialization of PCREF consists of four steps, including:

i) Cluster organization,
ii) Authentication information assignment,
iii) Key generation, and
iv) Local ID assignment,

i) Cluster organization

In this step they assign the cluster ID to each cluster and each sensing node stores its cluster ID, e.g. each sensing node in cluster i stores the cluster ID Ci in its memory. Each monitored node or component is monitored by n sensing nodes organized as a cluster. They can deploy n sensing nodes close to the monitored component. Those nodes communicate with each other and each node stores the node IDs of its neighbors to organize the cluster. The node ID is stored in the node before being deployed.

ii) Authentication information assignment

In this stage, they use the cluster-based primitive polynomial assignment mechanism to ensure that the primitive polynomial assigned for one cluster is different from others. The use of the ID-based polynomial generation ensures that the authentication polynomial and the check polynomial stored in one node are different from other nodes. This scheme leads to a high resilience to node impersonation attacks because the authentication information of one cluster has no impact on another cluster. The formation of authentication information in our scheme does not require node localization.

iii) Key generation

In this stage, by using the master key, each sensing node generates the cluster key. Notice that master key is erased once generation is completed. With the assumption that attackers cannot compromise node during initialization-phase, no one knows the master key even if attackers compromise nodes in filtering phase. Hence, master key are not globally known because that is in the encrypted form.

iv) Local ID assignment

With the use of the local ID, this scheme can detect the false measurement reports sent by the compromised cluster-head and increase the resilience to false data injection attacks. In this stage, each sensing node is assigned a local ID by its cluster-head. Cluster-head CHi sends the local ID assignment message to every nodes u in its cluster, After receiving the message, node u stores the local ID and sends the response message, The cluster-head collects all response messages and determines whether the n local IDs are assigned to the different cluster nodes. Note that n is the number of sensing nodes monitoring the physical component. If the cluster-head finds a local ID not being assigned, it repeats the above process and assigns it to a node.

4.1.2 Data Security Management

The data security management of PCREF consists of the sensing report generation, measurement report generation and transmission, en-route filtering, and controller authentication.

i) Sensing report generation

Each sensing node measures the data of the monitored component and generates the sensing report, which consists of the encrypted measurement, node ID, local ID, and MAP (Message Authentication Polynomial). Sensing nodes generate different MAPs for the same measurement using its node ID and locally stored authentication polynomial.

ii) Measurement report generation and transmission

After receiving all sensing reports generated by the sensing nodes, cluster-head randomly chooses T reports from them and merges these T measurement reports to an integrated measurement report R and sends it to controller.

A. The Proposed systems advantageous:

1. PCREF accomplish high elasticity against the large number of endangered nodes.
2. PCREF doesn't depend on static node i.e. node localization.
3. The compromised region proportion of PCREF is the minimum as compare to existing systems.
4. Good resilience against attacks.
5. Reduces manpower and Highly secured and easy to install
6. Better performance in wireless sensor network and Simple system & reliable

B. Mathematical Model and Algorithm: Polynomial-based bloom filtering

Input:

1. Set of Sensing nodes
   N = {S1, S2,……,Sn}.
2. Set of Forwarding node for sensing nodes i.e. cluster head.
   CH = {CH1, CH2,…..,CHn}.
3. Set of reports generated by sensing nodes at particular time stamp t.

   r = {r1, r2, ……., rn}.
4. Controller of the entire cluster heads who applies bloom filter on reports generated by sensing nodes.

Output: set of Authenticated reports {r1, r2, ….., rn},

Procedure:

1. All the nodes in the network are initialized w.r.to to a master key 'K', Master key is used to launch the key divided in between neighboring nodes in the every cluster.

Each node has been designate by a unique ID and each nodes stores IDs of that neighbors to form cluster. The node ID is stored in the node before it distributed. A network designer assign the cluster ID to each and every cluster and each sensing node hold its cluster ID, e.g., each and every sensing node in cluster CH*i* keep the cluster ID*Ci* in its memory.

After assigning IDs the nodes in the network are initiated.

{K, Kc, f(x,y,z),T, H(.)}.

Where,

- Kc is the set of master keys (central) in the clusters of nodes,
- f(x,y,z) Primitive polynomial of cluster *Ci* with parameter *x; y* and *z*.
- T is threshold set of polynomials.
- H is the hash function.

2. Authentication polynomial of node S1

auth (S1) = α f(S1, y, z),

3. Check polynomial of node S1

Verf (S1) = β f(S1, x, z).

4. Reports r1, r2, ……. , rn. are generated by

Report r = ((E)KCHi. — x — MAP)

5. MAP is Message authentication polynomial which is generated by each sensing nodes by,

MAP = authr(y, z) = α f(S1, y, H((E) Kc,))

Where,

- E = measured invigilator element,
- *H*(·) is the hash function hold in node Si
= *KCi* is the cluster key, to which *Si* belongs,
and the node Si creates MAP for the measurement.

6. Report along with MAP are sent to forwarding node.

7. Forwarding node performs polynomial based filtering and forwards report only if following conditions are satisfied.

Condition 1: The time stamp t connected to the report should be refreshing.
Condition 2: T MAPs connected in the result or report should be different and created by the sensing nodes.
Condition 3: T MAPs can be checked by the intermediate node using stored check polynomial.

8. Controller performs filtering same as forwarding node.

9. If report is valid, it decrypts and sends to respected cluster head.

10. Now, Polynomial Based filtering is performed by the cluster head and the controller i.e. admin. The en-route filter at controller marks '1' if particular sensor node is present (as like stored in check polynomial), else '0'. If it is ‘0’ then controller resolves that reports problem and then it forwards the filtered report to respected cluster head.

11. Membership/reports of nodes are checked each time the nodes forward report to the controller.

5. PERFORMANCE ANALYSIS

To get performance analysis of data transmission using novel en-route filtering scheme in cyber physical network we have three different graphs-

1. Packet delivery ratio
2. Energy consumption ratio

As the number of compromised nodes increases, the energy consumption of existing schemes increase rapidly, and the energy consumption of our scheme increase slowly and is lower than that of existing schemes.

In this case, the measurement report generated in the cluster can be forwarded to the controller within a few hops and be filtered by the controller, and the less that extra energy of intermediate nodes will be consumed during this process.

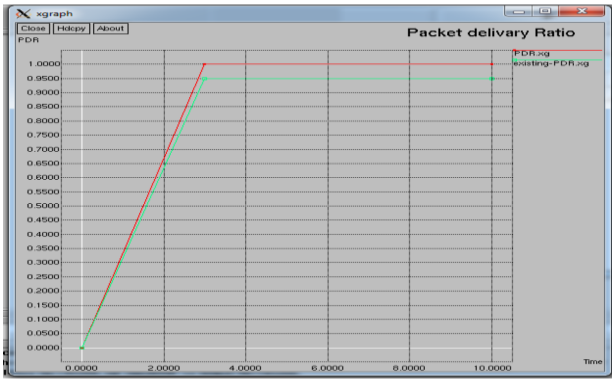

Fig 2: Packet delivery Ratio

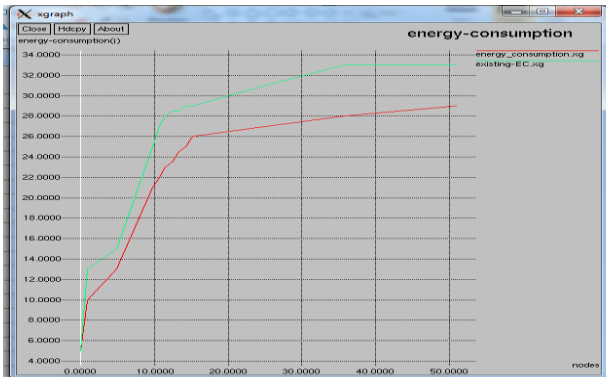

Fig 3: Energy consumption ratio

6. CONCLUSION

Performance analysis demonstrate that the designed system framework is fast to DETECT the deficiency i.e. fault and beat its issue. Proposed strategy is effectively actualized. Exhibited another class of attack, called false data infusion attack and a Polynomial-based Compromised-Resilient En-course Filtering approach, which filter false or incorrect data viably and accomplish eminent flexibility for the number of compromised nodes without depending on stable path and node determination. This system handle authentication information and separate the incorrect results measurement. PCREF receives polynomials for supporting estimation reports to enhance versatility to the node impersonating attacks.

7. REFERENCES

[1] Xinyu Yang_, Jie Lin_, Paul Moulemay,Wei Yuy, Xinwen Fuz and Wei Zhaox “A Novel En-route Filtering Scheme against False Data Injection Attacks in Cyber-Physical Networked Systems” IEEE Transction on computers, VOL. 64, No. 1, January 2015.

[2] Y. S. Chen and C.L. Lei, “filtering false messages en-route in wireless multi-hop networks,” IEEE, wireless communication network conference, 2010, pp. 1-6.

[3] Z. Yu. And Y. Gaun, “A dynamic en-route filtering scheme for data reporting in wireless sensor networks,” IEEE Trans networking, Vol. 18, pp. 150-163, 2010.

[4] S. Zhu, S. Setia, “An interleaved hop-by-hop authentication scheme for filtering of injection false data in sensor networks,” ACM Trans sensor Network, Vol. 3, no. 4, pp. 259-271, 2007.

[5] T. Yuan, S. Zhang, “An en-route scheme of filtering false data in wireless sensor networks,” IEEE Int. perform. Comput. Commun. Conf. pp. 193-200, 2008.

[6] L. Yu and J. Li. Grouping-based resilient statistical en-route filtering for sensor networks. In Proc. of the 28th IEEE INFOCOM, 2009.

[7] F. Wu, Y. Kao, and Y. Tseng, “from wireless sensor networks towards cyber physical system,” Pervasive mobile comput., Vol. 7, no. 4, pp. 397-413, Aug. 2011.

[8] H. Yang and S. Lu. “Commutative cipher based en-route filtering in wireless sensor networks”. In Proc. of 60th IEEE VTC, 2004.