Improved Resilience against False Data Injection Attacks using PCRE Filtering Scheme

J. Mamsa
Dept. of CSE
Easwari Engineering College
Chennai, India

A. Kalaiarasi
Dept. of CSE
Easwari Engineering College
Chennai, India

Mrs. S. Kalpana Devi
Dept. of CSE
Easwari Engineering College
Chennai, India

***Abstract* - Cyber physical system is a system of collaborating computational elements controlling physical entities. The development of cyber physical networked system can sense and affect their environment in different ways and with different levels of sophistication. To resolve this issue, the en-route filtering schemes are designed for wireless sensor networks. In wireless sensor network an adversary may crack legal nodes or deploy malicious nodes to launch various attacks. These nodes are collectively called as compromised nodes. Once the sensor gets compromised, the security of the network degrades quickly. In our work, we propose a Polynomial- based Compromised-Resilient En-route filtering scheme for achieving a high resilience by using authentication polynomial and check polynomial without relying on static routes and node localization.**

Keywords* - *wireless sensor network, compromised nodes, resilience, polynomial based en-route filtering, node localization.

I. INTRODUCTION

Monitoring and controlling physical systems through distributed sensors and actuators have become an essential task in environment and infrastructure applications. These applications have received a renewed attention because of the advances in sensor network technologies and new development in cyber physical networked systems. Cyber physical systems (CPS) are complex engineering systems that rely on the integration of physical, computation, and communication process to function.

Advances in this field will have great technical, economic and societal impacts in the near future. A wireless sensor network is a group of specialized transducers with a communication infrastructure that uses radio to monitor and record physical or environmental condition. The network provides a bridge between the real physical and virtual worlds and have a wide range of potential applications to industry, science, transportation, civil infrastructure, and security. Cyber –Physical Systems (CPS) are next-generation embedded systems featuring a tight integration of computational and physical element. Emerging applications of CPS include transportation, healthcare, energy, manufacturing, entertainment, aerospace, etc., all of which will be essential pieces of our social infrastructure. In cyber physical networked systems (CPNS), the sensor nodes obtain the measurement reports from the physical components, process the measurements and send measured data to the controller through networks.

The sensor node is a node in wireless network that is capable of performing some processing, gathering sensory information and communicating with other connected nodes in the network. To facilitate unprecedented interactions between human beings and the physical world, sensor networks become a crucial ingredient of CPNS due to the need for coupling geographically distributed computing devices with physical elements.In real world the adversary can use the wireless devices to connect tothe CPNS or compromised Physically capture sensor nodes through code injection attacks or node replication attacks, in which the adversary can

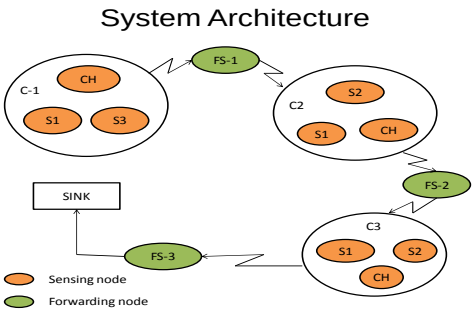

Fig 1: System model for Filtering Scheme

physically captures some of the nodes in the network and collect all credential like key, identity, etc., then reprogram or replicate it in order to eavesdrop the transmitted message or compromise the functionality of the networks. This causes the controller to estimate wrong system state and posses dangerous threats to the systems. The false reports consume a lot of network and computational resources and shorten the life time of sensor networks and CPNS. Hence to ensure the normal operation of the system it is critical to filter false data at forwarding nodes before arriving at the controller.

In the past, the number of schemes has been designed to filter the false injected data in sensor networks. However those schemes have their limitations and cannot used to effectively deal with attacks related to CPNS. So, we propose a polynomial based compromised resilient en-route filtering scheme (PCREF) for CPNS, which can filter false data effectively and achieve a high resilience.Figure 1 specifies the system model for filtering the injected false data effectively through the number of sensor nodes and forwarding nodes with highest resilience. Resilience is the ability of the network to provide and maintain acceptable

level of service in the face of various faults and challenges to normal operation. Thus the resilient network aims to provide acceptable service to applications.

II. ALGORITHM

A. Introduction

Generally in en-route filtering scheme, intermediate nodes are used to check the authenticity of messages and filter them when those messages travel through the network. The basic idea of our scheme is to use polynomials instead of MACs to verify reports, and can mitigate the node impersonating attack against legitimate nodes. By grouping the nodes into clusters the security is assured to the nodes, where the adversary's compromised nodes in one cluster will not affect the security of other clusters. The nodes in the cluster are responsible for same monitored components and the PCREF assigns the corresponding authentication polynomials and check polynomials to each sensor nodes. The authentication polynomial stored in each node is used to endorse the report of local component measurement, while the check polynomial is used to validate the report. These polynomials stored in nodes are bundled with node id and derived by the primitive polynomials assigned from a primitive polynomial pool. In the cluster based primitive polynomial assignment, nodes in different clusters are assigned different primitive polynomials from the global primitive polynomial pool and generate different authentication polynomial and check polynomial. Each sensing nodes stores the authentication polynomial of the local cluster and stores the check polynomial of other cluster with a predefined probability P. The probability P is used to measure the acceptable probability of sharing authentication information between two nodes.

B. Pseudo code

The master key is generated and stored in the memory of sensor nodes before they are deployed and used to produce the cluster key for each cluster. The primitive polynomial is assigned to each cluster and its size is l(l<Ns/n), where n is the number of sensing nodes monitoring a component, Ns is the total sensing nodes in the system.

Step 1: Cluster organization: Each monitored component is monitored by n sensing nodes are organized in a cluster. Each sensor node contains the node ID of other sensing nodes in its cluster before it is deployed. Each cluster has its own cluster ID and is stored in each sensing nodes of that cluster.

Step 2: Authentication Information Assignment: In this step, all nodes are initialized by the network designer with the parameters mentioned below:

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

Where Kc is the master key, f(x, y, z) is the element from a set of polynomials, T is the threshold, and H(.) is a hash function, and x, y, z are unknown parameters. The parameter x represent the sensing node ID and the parameter y represent the forwarding node ID and the parameter z represents all the measurement reports of monitored components. For each sensing node u, the network designer stores the master key Kc and the hash function H(.). The network designer evaluates the authentication polynomial of cluster C_i for each sensing node u by

$$\text{Auth}_i{}^u(y,z)=\alpha f_i(u,y,z),$$

Where x,y,z are parameters, u is the sensing node ID in cluster C_i,$f_i(x,y,z)$ is the primitive polynomial of cluster, $\text{auth}_i^u(y,z)$ is the authentication polynomial of cluster and $\alpha \in \{,2^2,2^2,2^4,2^5\}$. The value of α is chosen randomly by the system designer during the computation of authentication polynomial to increase the resilience. The α value is not known to the other party, so that no other party can extrapolate the authentication polynomial of the clusters. The designer then computes the check polynomial with the probability p for each cluster. For each forwarding node w, the designer computes the check polynomials ver fju(x,z) of all clusters with probability p and stores hash function H(.) and stores these check polynomials in node u by

$$\text{Ver } f_j^u(x, z) = \beta\ f_j(x, u, z),$$

Where $\text{Ver } f_j^u(x, z)$ is the check polynomial of cluster C_j stored in node u, $\beta \in \{2^5, 2^6, 2^7, 2^8\}$ and it plays the same role as α.

Step 3: Key Generation: In this stage, by using the master key K_C, each node generates the cluster key. The cluster key of cluster C_i stored in each sensing node is denoted as,

$$K_{Ci} = F_C(K_C \mid CH_i)$$

Where CH_i is the cluster head ID and | is denoted as the concatenation operation and its function is to combine two strings to one string, $F_C(*)$ is the cluster key generation function. The above equation shows the concatenation of string K_C and CH_i to one new string, and then uses the new string to generate the cluster key K_{Ci}.

C. Performance

After receiving all sensing reports generated by the sensing nodes, the cluster-head randomly chooses T reports from them and merges these T measurement reports to an integrated measurement report R and sends it to the controller. Then the cluster-head sends R to the controller through the intermediate nodes along the route. Because of the broadcast nature of wireless communication, the sensing nodes in the same cluster also eavesdrop the measurement report sent by cluster-head and determine:

i. T local IDs included in R.
ii. The information attached in R is the same as ones stored in each sensing node with local ID.

If the above two conditions are not satisfied sensing nodes will send the warning message to the first intermediate

node and request it to drop report R. Otherwise no warning message will be sent.

In PCREF scheme only the first intermediate node that receives the report from the cluster-header needs to receive the warning message to detect whether the local ID attached in the report is legitimate. Hence, to ensure the warning message reaches the first intermediate node before it reaches the next intermediate node, the first intermediate node should wait a few clock cycles for receiving the warning messages after receiving the measurement reports. If there is no arrival of warning messages till the completion of the clock cycles, then the first intermediate node will forward the measurement report. The number of clock cycles is predefined and the waiting time ensures that the sensing node can complete the decision and send out the forwarding message. In this way PCREF can drop the forged data effectively. Depending on the Nature of monitored physical systems the sensing nodes can only be on when they need to monitor the state of the components, and sensing nodes can enter the sleep mode to save energy as well. The forwarding nodes can leverage the existing duty-cycle schemes to switch on/off and save energy. The communication scheme and routing protocols developed in the past can be leveraged to establish routes to forward the measurement reports through forwarding nodes. PCREF scheme can be used in forwarding nodes on the route to forward and validate the measurement reports.

III. TECHNIQUE

By leveraging the polynomial based message authentication introduced in, PCREF conducts the en-route filtering on false measurement reported from the compromised nodes while the existing approaches cannot do so. In PCREF the measurement report transmitted to the controller hop by hop. The intermediate node which does not have the corresponding check polynomial associated with the cluster, where the measurement is originally generated (e.g., cluster ID is attached in the report), forwards the measurement report to the next node along the route. The intermediate node, which has corresponding check polynomial, determines whether the received measurement report R is false through validating the following conditions.

Condition 1: The time as timestamp attached in R is fresh.

Condition 2: T MAPs attached in the report are different and are generated by the sensing nodes in the corresponding clusters where cluster ID is claimed in the report.

Condition 3: T MAPs can be verified by the corresponding check polynomial stored in the intermediate node.

If the conditions are not satisfied the intermediate node will drop the measurement report, otherwise the measurement report will be forwarded. The timestamp denoted as time field in the message can specify the time when the measurement reports are generated in the monitored component. The forwarding nodes and controller can determine whether the received reports is the newest generated one, i.e.., whether it is fresh. Hence, the condition 1 uses the time as timestamp to determine the freshness of the forwarded measurement reports and detect the replayed false report .To verify the condition 2 and condition 3 the intermediate node first calculates the values of $A_i^{um,v}$and $V_i^{u,um}$ while the value of z calculated by equation(6),

$$A_i{}^{u}{}_{m}{}^{,v}=auth_i{}^{u}{}_{m}(v,H((E)_{kci})),$$

$$=\alpha f_i(u_m,v,H((E)_{kci)),}$$

$$V_i{}^{v,u}{}_{m} =verf_i{}^{u}(u_m,z)=\beta f_i(u_m,v,z),$$

$$= \beta f_i(u_m,v,H((E)_{kci})),$$

Where v is the node ID of the intermediate node, u_m is the sensing node ID carried in the report, $auth_i^{um}(y,H((E)_{kci}))$,is the MAP generated by u_m and is included in the report, $verf_i^v(x,z)$ is the check polynomial of cluster C_i stored at node v. In existing system the RSA algorithm is used for secure encryption and decryption using asymmetric key system in wireless sensor nodes during data transmission. But while using the asymmetric key system also the attacker can find the private key used for decryption. So in our scheme we improved the security by using AES (Advanced Encryption Standard) algorithm. In AES 128 bit key is used for encryption and decryption while in RSA separate keys are used for encryption and decryption.

IV. IMPLEMENTATION

In this paper, we proposed a Polynomial Based Compromised Resilience en-route Filtering scheme for filtering false data injection attacks and DoS attacks in wireless sensor networks. In this scheme, each node uses its own authentication polynomial to authenticate the forwarding reports and a legitimate report should be endorsed by nodes. The cluster-head disseminates the first auth-key of every node to forwarding nodes and then sends the reports to the controller. The data is encrypted for security purpose using RSA and AES algorithm. The forwarding nodes verify the authenticity of the forwarded reports and then check the integrity and validity of the reports using the authentication and check polynomial assigned to the nodes. According to the verification results, they either drop or keep on forwarding the reports. This process is repeated by

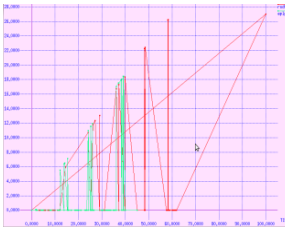

Fig 2: Data Loss

Fig 3: Throughput workload

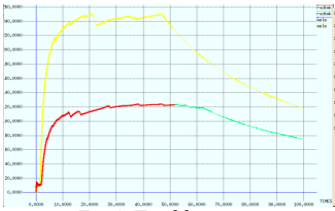
Fig 4: Total losses

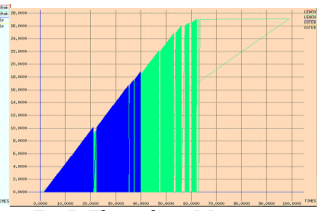
Fig 5: Throughput Measurement

each forwarding node at every hop. Amajor challenge in a Wireless Sensor Network lies in the energy constraint at each node, which poses a fundamental limit on the network life time. Figure 2 shows data loss reports of existing system and proposed system. In proposed system data loss is reduced from 100% to 40%. Figure 3 shows reducing throughput workload in proposed system. Due to reduced data loss the total loss is also reduced. This is shown in figure 4. The increasing throughput measurement is shown in figure 5. Even though there are many en-route filtering schemes available in the literature they either lack to support the dynamic nature of the sensor networks or they cannot efficiently mitigate the adversaries' activities. Hence this Polynomial Based Compromised Resilience En-route filtering scheme is currently an area of much research among the security professionals. Because, this Filtering schemefollows the dynamic routing and also highly resilient.

V. PERFORMANCE DISCUSSION

The filtering efficiency is defined as the ratio of filtered false measurement reports within a forwarded hop. Filtering capability is calculated by the average forwarded hops, where the false measurement report is forwarded until being filtered. The resilience can be evaluated by the ratio of total compromised components versus the probability of components those measurement reports can be successfully forged by the adversary. We prove that the adversary cannot forge a report since authentication and check polynomial information assigned by the system designer is not known to the adversaries.

An Analytical and simulation result shows that PCREF achieves the highest ratio of filtered false measurement reports while other filtering scheme achieves the worst performance. The smaller the number of hops used for report forwarding, the greater the filtering capacity. Figure 2 and figure 3 shows the average hops that the measurement reports are forwarded versus the number of compromised sensing nodes in terms of analysis and simulation respectively. As we can see, when the number of compromised sensing nodes increases, the average forwarded hops of PCREF increases slowly while it increases rapidly for other schemes. The existing schemes introduce node localization and node associations based on statically configure routes or conforming to beam model [26]. This takes a longer time to stabilize with a large amount of network resource energy consumption, and they are highly vulnerable to malicious attacks. All these limits reduce the performance of CPNS (Cyber Physical Network System). But the PCREF scheme achieves better performance than existing schemes by using the RSA and AES algorithm. For example, the filtering efficiency of PCREF increases as the forwarded hops increases, and it is always greater than that of existing schemes. In terms of filtering capability, given a network with 10000 nodes, within seven forwarded hops even if 20 percent of sensor nodes are compromised, PCREF can filter false data effectively while other schemes can lose the entire en-route filtering capability. In addition, the average number of forwarded hops of PCREF increases slowly as the size of network increases. With the same number of compromised nodes, the compromised area ratio of PCREF is the lowest while comparing with the existing schemes. This scheme detects the modified report effectively with high resilience. Also the existing schemes cannot deal with forged reports injected by comprised nodes, because the adversary can obtain the authentication polynomial stored in the compromised nodes and successfully forge valid authentication information attached in the reports. This causes the intermediate nodes to fail in filtering false messages. But in our scheme, this can be avoided as we are using the RSA and AES algorithm for secure encryption and decryption so it filters the forged reports also. But it still cannot achieve 100% results in filtering the forged reports.

VI. CONCLUSION

Security is serious factor for many sensor networks, because of the limited capabilities of sensor nodes. Even though there are many mechanisms available to explain about the security for wireless sensor networks, offering security and privacy to a sensor network is a difficult task. The filtering scheme is one of the secure mechanisms in wireless sensor networks. It provides security in Wireless Sensor Networks by identifying some of the attacks. One of the drawbacks of en-route filtering scheme is that it can filter 80% of false measurement reports only. To improve the efficient filtering in WSN an efficient polynomial based Compromised Resilience En-route Filtering Scheme is used here. This filtering scheme is used to filter the information of the compromised node. Through this filtering scheme we can identify the injected false data report attack and provide secure mechanism for data reporting. When we identify the false data report it can also reduce the energy consumption and communication overhead. In the future work, the performance of this filtering scheme will be analyzed under different routing protocols.

REFERENCES

[1] Yao-Tung Tsou, Chun-Shien Lu, Sy-Yen Kuo, "MotesecAware: a practical secure mechanism for wireless sensor network," IEEE Trans. On Wireless Communications, vol. 12, no.6, pp. 2817-2829, 2013.
[2] C. M. Yu, Y. T. Tsou, C. S. Lu, and S. Y. Kuo, "Constrained function based message authentication for sensor networks," IEEE Trans. Inf. Forensic and Security, vol. 6, no. 2, pp. 407-425, 2011.
[3] A. Perrig, R. Szewczyk, V. Wen , D. Culler, and J. D. Tygar, "SPINS: security protocols for sensor networks," in Proc. 2001 International Conference on Mobile Computing and Networking, pp. 189-199.
[4] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route detection and filtering of injected false data in sensor networks," in Proc. IEEE INFOCOM, 2004, vol. 4, pp. 2446-2457

[5] S. Zhu, S. Setia, and S. Jajodia, and P. Ning, "An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks," in proc. IEEE Symp. Security Privacy, 2004, pp. 259-271.
[6] Giruka. V. C, Singhal.M, Royalty. Y , and Varanasi.S, (2007) "Security in Wireless Sensor Networks," Wireless Comm. and Mobile Computing, vol.8, no. 1, pp. 1-24.
[7] Yu.C.M, Lu.C.S, and Kuo S.Y, (2005) "A Dos-Resilient En-Route Filtering Scheme for Sensor Network," Proc. Tenth ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc'09), pp. 343-344.
[8] S. Kun, L. An, N. Peng, and M. Douglas, "Securing network access in wireless sensor networks," in Proc. 2009 International Conference on Wireless Network Security, pp. 261-268.
[9] B. Przydatek, D. Song, and A. Perrig, "SIA: Secure information aggregation in sensor networks," in Proc. ACM SenSys, 2003, pp. 255-265.
[10] D. He, J. Bu, S. Zhu, S. Chan, and C. Chen, "Distributed access control with privacy support in wireless sensor networks," IEEE Trans. Wireless Commun., vol. 10, no. 10, pp. 3472-3481, Dec. 2011.
[10] Z. Yu and Y. Guan, "A dynamic en-route scheme for filtering false data injection in wireless sensor networks," in Proc. IEEE INFOCOM, 2006, pp. 1-12.
[11] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient security mechanisms for large- scale distributed sensor networks," in Proc. ACM CCS, 2003, pp.62-72.
[12] H. Yang and S. Lu, "Commutative cipher based en-route filtering in wireless sensor networks," in Proc. IEEE VTC, 2004, vol. 2, pp.1223-1227.
[13 C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," in Proc. 1st IEEE Int. Workshop Sensor Netw. Protocols Appl., 2003, pp. 113-127.
[14] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, "Toward resilient security in wireless sensor networks," in Proc. ACM MobiHoc, 2005, pp. 34-45.