INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

AN EN-ROUTE SCHEME OF FILTERING DATA IN WIRELESS SENSOR NETWORK

Siva Prakash T[1], Kadhirvelu D[2]

[1]*M.E. CSE student, Krishnasamy College of engineering and technology,*
E-mail id: sivaprakash9001@gmail.com
[2]*Associate Professor, Krishnasamy College of engineering and technology,*
E-mail id: siva_thenaughty07@yahoo.co.in

Abstract

Monitoring and controlling physical systems through geographically distributed sensors and actuators have become an important task in numerous environment and infrastructure applications. Unlike more traditional embedded systems. The existing en-route filtering schemes are based on T authentication, i.e., a legitimate measurement report must carry at least T valid message authentication codes (MACs) generated by different valid sensor nodes in CPNS, where T is the threshold and predefined before CPNS is deployed. When a report is transmitted from a sensor node to the controller, each forwarding node checks whether the forwarding reports actually carry T valid MACs. If not, the report is considered as a false one forged by the adversary and then dropped. Otherwise, the report is forwarded to the next forwarding nodes along the route. In our proposed system, we propose a Polynomial-based Compromise- Resilient En-route Filtering scheme (PCREF) for CPNS, which can filter false injected data effectively. PCREF adopts polynomials instead of MACs (Message Authentication Codes) to verify reports, and can mitigate node impersonating attacks against legitimate nodes. In our scheme, two types of nodes are considered, they are sensing node and forwarding node. These two types of nodes are denoted as sensor nodes. Each node stores two types of polynomials: authentication polynomial and check polynomial, which are derived by different primitive polynomials. The sensing node can not only sense and endorse the measurement reports of the monitored components, but also forward the measurement reports along the route. The forwarding node is used to forward the received measurement reports to the controller.

Keywords*:* Cyber-physical networked system, Data injection attack, sensor networks, and polynomial-based en-route filtering.

1. Introduction

Wireless sensor networks sense the data through sensors and transmit the sensed data from one node to another node. CPNS, consisting of sensor nodes, actuators, controller, and wireless networks, have been widely used to monitor and affect local and remote physical entities in the physical world. Typical CPNS cover a wide range of applications including transportation networks, vehicular networks, networks of unmanned vehicles and so on. [1]. Sensors gather information about the state of physical world and transmit the collected data to actuators through single-hop or multi-hop communications over the radio channel. [2]. Cyber-Physical Systems (CPS) integrates computing and communication capabilities with monitoring and control of entities in the physical world. a Polynomial-based Compromised-Resilient En-route Filtering scheme (PCREF), which can filter false injected data effectively and achieve a high resilience to the number of compromised nodes

without relying on static routes and node localization. Particularly, PCREF adopts polynomials instead of MACs (message authentication codes)for endorsing measurement reports to achieve the resilience to attacks. Each node stores two types of polynomials: authentication polynomial and check polynomial derived from the primitive polynomial, and used for endorsing and verifying the measurement reports. Via extensive theoretical analysis and simulation experiments, our data show that PCREF achieves better filtering capacity and resilience to the large number of compromised nodes in comparison to the existing schemes.[1].

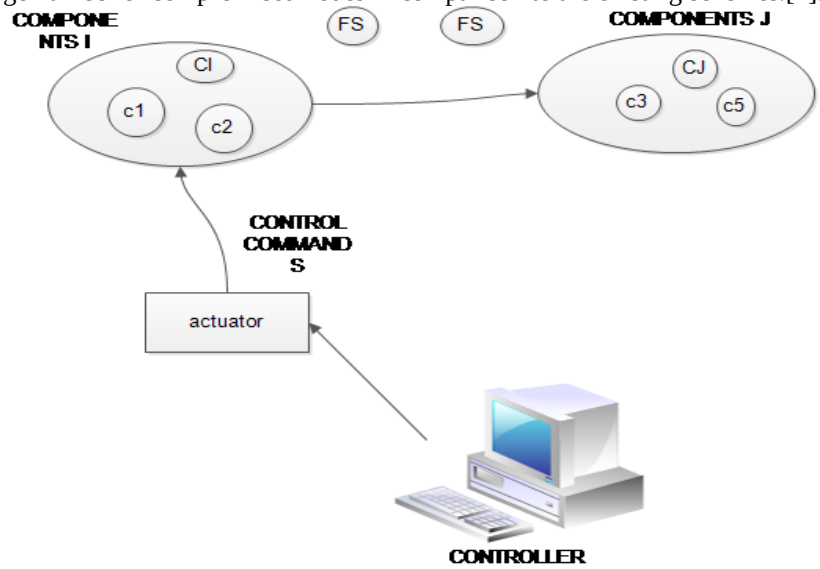

Figure 1 : System Model

2. Related Works

We (1) identify and define the problem of secure control, (2) investigate the defenses that information security and control theory can provide, and (3) propose a set of challenges that need to be addressed to improve the survivability of cyber-physical systems[4]. The requirements for immersive cyber physical systems in. which people interacts with their local environments. Trusted Platform Module (TPM) can make it possible to include sophisticated security provisions in an RPL implementation. It presents how it would be possible to use the security mechanisms of a TPM in order to secure the communication in an RPL network[5].

3. Proposed System

CPNS is used to receive measurements from sensor nodes, estimate system states, and send commands to the actuators to control the operation of physical systems. Each physical component or system is measured by multiple sensing nodes to increase resilience to faults and the nodes that measure the same component are organized as a cluster. A number of nodes in the cluster collect measurements and send data to the controller via multiple hops. To simplify our analysis, we assume only one controller in the system. Nodes may be mobile and nodes within the same cluster are relatively static to each other. There are two types of nodes in the system: sensing nodes and forwarding nodes and these two types of nodes are denoted as sensor nodes in the paper, represented as green nodes and blue nodes in Fig. 1, respectively. The sensing node can not only sense and form the measurement reports of the monitored components, but also forward the measurement reports of other nodes. The forwarding node can only forward the measurement reports to the controller. We assume that each cluster has a unique cluster ID and each node has a unique node ID. Sensor nodes that measure or forward measurement reports have a limited computation and communication capability and limited energy resources. Sensor nodes lack tamper-resistance hardware and can be compromised by attackers. Fig. 1 shows the example of system model, where node v1,v2,v3 and v4 obtain the measurement reports of monitored component j and send them to the controller via v4. Similarly, u4 sends the measurement report of monitored component i to the controller through multiple forwarding nodes. We can see that v1 can serve as a forwarding node to transmit the measurement reports of monitored component i. We assume that the attacker can compromise sensor nodes, including both the sensing nodes and forwarding nodes. Once a node is compromised, the secret information stored in the node becomes visible to the attacker. The attacker can inject false measurement reports to the controller via the compromised nodes. This causes the controller to estimate wrong system states

and send wrong control commands to the actuators, posing the dangerous threats to the system. The false reports also consume lots of network and computation resources and shorten the lifetime of CPNS. We assume that the controller is well protected and the attacker could only obtain the authentication information through compromising sensor nodes. We also assume that there is a reliable node initialization after nodes being deployed, and the attacker cannot compromise or damage any node during the initialization phase. We restrict the forged data to the sink node and drop that data at the receiving node itself when that data is Identified as false.

3.1 Network topology

Each node sends "hello" message to other nodes which allows detecting it. Once a node detects "hello" message from another node (neighbor), it maintains a contact record to store information about the neighbor. Using multicast socket, all nodes are used to detect the neighbor nodes.

3.2 Cluster Updating and Key Distribution:

In a cluster, each monitored component is monitored by *n* sensing nodes and it can communicate with each other nodes. We assign the cluster name to each cluster and each sensing node stores its cluster name. Each cluster can communicate with the help of forwarding sensors. Each sensing nodes can sense the data and forward the data to the forwarding sensors. Then the measured data can be forwarded to the controller with the help of forwarding nodes. Each sensing node stores the stores the check polynomial of other clusters. Data can be validated by using this check polynomial.

Serious security threat is originated by node capture attacks in hierarchical information aggregation wherever a hacker achieves full management over a sensing element node through direct physical access in wireless sensing element networks. It makes a high risk of knowledge confidentiality. Data aggregation is defined as the process of aggregating the data from multiple sensors to eliminate redundant transmission and provide fused information to the base station. The main goal of data-aggregation algorithms is to gather and aggregate data in an energy efficient manner so that network lifetime is enhanced. Data aggregation helps in improving the performance of the wireless sensor network protocols especially the routing protocols which in turn improve the overall performance of the network. WSNs have many constraints including energy, redundant data, and many-to-one flows.

Data aggregation is one of the most important issues for achieving energy-efficiency in wireless sensor networks. Sensor nodes in the surrounding region of an event may generate redundant sensed data. A data aggregation technique in WSNs focuses on decreasing the energy consumption by reducing the amount of data that needed to be sent to the sink node.

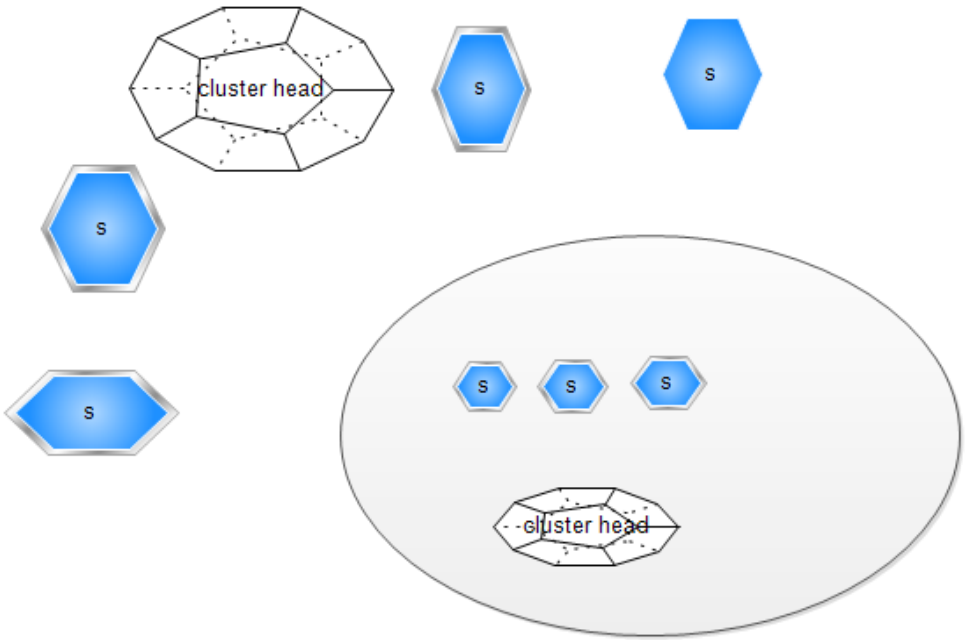

Figure 2: Cluster view of system model

4. Architecture

Nodes are formed as different clusters. Each cluster has different sensors nodes and the data has been transmitted from one cluster node to another cluster node from the cluster head to another cluster head through the forwarding sensors. Cluster head has been chosen with the priority of nodes battery and memory. And the data has been finally transmitted to the sink node.

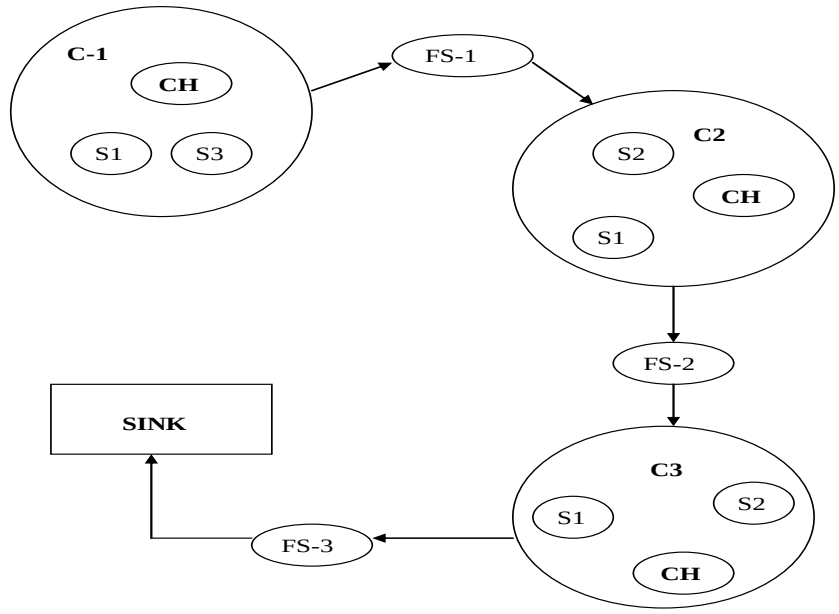

Figure 3 : Architecture diagram

5. Implementation

The basic idea of our scheme is described below. PCREF uses polynomials instead of MACs to verify reports, and can mitigate the node impersonating attack against legitimate nodes. By organizing a set of sensing nodes into a cluster, where nodes are responsible for the same monitored components, PCREF assigns the corresponding authentication polynomial and check polynomial to each sensor node. These polynomials stored in nodes are bundled with node ID and derived by the primitive polynomials assigned from a primitive polynomial pool. Different primitive polynomials will be used in different clusters through the cluster-based primitive polynomial assignment. This increases the resilience of our scheme to the increasing number of compromised nodes without relying on the node localization and static data dissemination routes. 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 received reports. Each sensing node stores the authentication polynomial of the local cluster and stores the check polynomial of other clusters with a pre-defined probability P. Each forwarding node stores the check polynomial of each cluster with the same probability P. Our scheme also uses T-authentication framework similar to [1],[2],[3] i.e., a legitimate report shall be authenticated by T nodes from the same cluster. Forwarding node could verify the report only if it shares the authentication information with the source node. Our scheme consists of the following two key components: (i) authentication information management is used to assign the key, authentication polynomial, check polynomial, and local ID of sensing nodes, and (ii) data security management is used to detect and filter the false measurement reports.

6. Result

In a cpns a data has been sent and that data is received only by the neighbour node so that the range of the

networked systems is visible. In our evaluation setting, we consider the scenario of 100 components and 1000 sensing nodes (i.e., each component is monitored by 10 sensing nodes). To make the scenario suitable for LBRS and LEDS, we consider that components form a 10 ∗ 10 array and are deployed in a [0,500m] × [0,500m] area uniformly, i.e., each component is deployed in a square with side length of 50m. The controller is located at (0,0). The cluster used in PCREF, responsible for monitoring the component is similar to the cell used in LBRS and LEDS. We also set T = 5, n = 10, and the node communication radius Rt = 50m. For SEF, GRSEF, LBRS and PCREF, the key sharing probability or the check polynomial sharing probability q is 0.2. In each simulation, a number of sensing nodes are randomly selected as the compromised nodes. The filtering efficiency is evaluated by the ratio of filtered false measurement reports within forwarded hops. Filtering capability is evaluated 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 vs. the total number of components, that is, the probability of components those measurement reports can be successfully forged by the attacker. For PCREF, LEDS and LBRS, the ratio of compromised components can be obtained based on the definition. For GRSEF, we check whether the attacker can forge a valid report from each grid-point by dividing the area into virtual grids. The resiliency of SEF is evaluated by the times for obtaining T keys successfully from distinct partitions by the attacker vs. total number of experiments. Note that, For the MAP forging successful ratio mentioned in section IV, it just to prove that the attacker could not forge a legitimate MAP with no knowledge of authentication information revealing to him, could not need to be simulated. Hence, we don't simulate it in this section. Each simulation is repeated 100 times and the simulation result shows the average value over 100 times. 1) Filtering Efficiency: it shows the analytical results of the ratio of filtered false measurement reports vs. the number of forwarded hops of SEF, PCREF, LEDS, GRSEF and LBRS. It shows the simulation results of those schemes, when 100 sensing nodes (i.e., 10% the total number of nodes) are compromised by the attacker. As we can see, both the analytical and simulation results constantly show that PCREF has the highest ratio of filtered false measurement reports and SEF achieves the worst performance. The filtering efficiencies of GRSEF, LBRS, and LEDS are always lower than that of PCREF. 2) Filtering Capability: it show the average hops that the measurement reports are forwarded vs. the number of compromised sensing nodes in term 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 others increase rapidly. When the number of compromised sensing nodes is less than 30 (i.e., 3% of the total number of nodes), the average forwarded hops of PCREF is one hop larger than that of LBRS and LEDS. The reason is that LBRS and LEDS rely on the static routes and achieve higher filtering efficiency within first several forwarded hops. However, the specific routes make LEDS and LBRS vulnerable, because once the attacker damages the route (e.g., jamming), the measurement report could not be transmitted to the controller on time, posing the degradation of system performance. Resilience: it show the analytical results of the ratio of successful times in SEF and the percentages of compromised components (cells or clusters)of GRSEF,LBRS, LEDS, and PCREF given the total number of compromised sensing nodes of 200 and 500, respectively. It shows the simulation results.

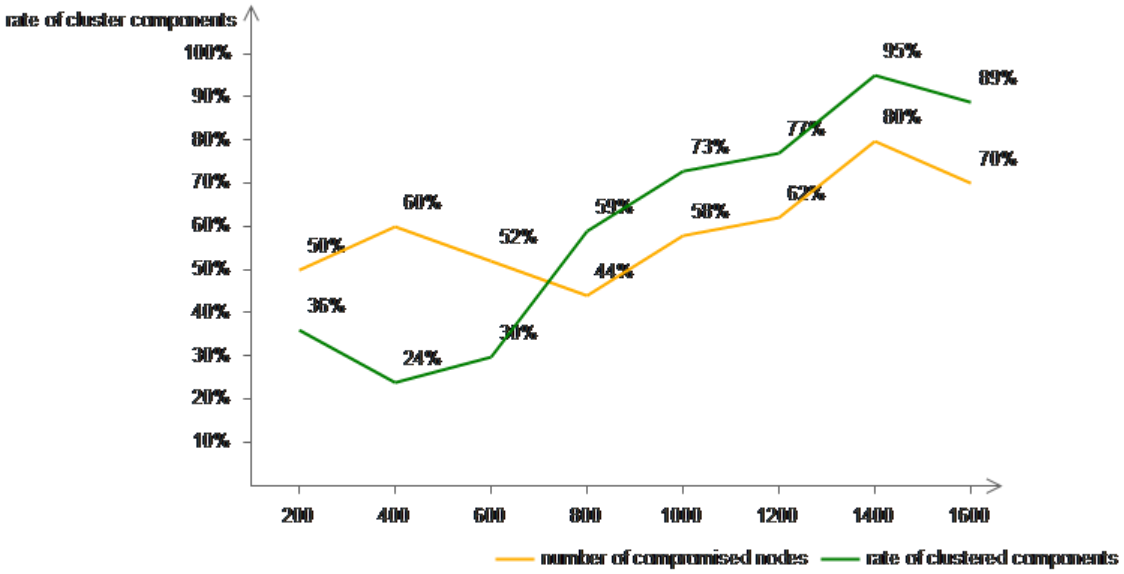

Figure 4 : Performance evaluation

7. Conclusion

In this paper, we proposed a Polynomial-based Compromised-Resilient En-route Filtering scheme (PCREF), which can filter false data effectively and achieve high resilience to the number of compromised nodes without relying on static routes and node localization. PCREF adopts polynomials for endorsing measurement reports to improve resilience to the node impersonating attacks. Each node stores two types of polynomials: authentication polynomial and check polynomial derived by primitive polynomial, and used for endorsing and verifying the measurement reports, respectively. We develop techniques to effectively manage authentication information and filter out the false measurement reports. Via both theoretical analysis and simulation experiments, our data show that our schemes achieves better filtering capacity and resilience to the large number of compromised nodes in comparison with the existing schemes. And also we ensure that the false data has been filtered at the very next node. We sent a dummy data over the network and the time calculated of the data send and receives so that the approximate time also evaluated so that the forged data of chance can also be identified.

REFERENCES

[1] Yang, Xinyu, et al. "A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems." *Distributed Computing Systems (ICDCS), 2012 IEEE 32nd International Conference on*. IEEE, 2012.
[2] Xia, Feng, Xiangjie Kong, and Zhenzhen Xu. "Cyber-physical control over wireless sensor and actuator networks with packet loss." *Wireless Networking Based Control*. Springer New York, 2011. 85-102.
[3] Seeber, Sebastian, et al. "Towards a trust computing architecture for RPL in Cyber Physical Systems." *CNSM*. 2013.
[4] Karim, Md E., and Vir V. Phoha. "Cyber-physical Systems Security." *Applied Cyber-Physical Systems*. Springer New York, 2014. 75-83.
[5] Seeber, Sebastian, et al. "Towards a trust computing architecture for RPL in Cyber Physical Systems." *CNSM*. 2013.