IOSR Journal of VLSI and Signal Processing (IOSR-JVSP)
e-ISSN: 2319 – 4200, p-ISSN No. : 2319 – 4197
PP 41-46
www.iosrjournals.org

A Reliable Scheme To Filter False Data At Minimial Hops For Secured Wsn

V.Laya Priya[1], G.Sudha[2]
[1](Post graduate student, Electronics and communication, Sri Sairam engineering college,India)
[2](Assistant professor-1, Electronics and communication, Sri Sairam engineering college,India)

Abstract : *Wireless Sensor Network has been widely used in various application areas like patient care, habitat monitoring, sensing physical parameters, traffic monitoring and so on. WSN integrates computing, communication and storage capabilities with monitoring and control of entities in the physical world, and must do so dependably, safely, securely, efficiently and in real-time. Sensor nodes obtain the measurement from the physical components, process the measurements and send measured data to the controller through networks. According to measurements, the base station estimates the state of physical systems and sends feedback commands to control the operation of physical systems. The attacker can infuse false data to the system through compromised sensor nodes which eventually weaken the system's security. To address the above issue few en-route filtering schemes exist but they lack resistance to the number of compromised nodes. The planned scheme endorses data at each hop before forwarding it to the next node which ensures detecting false data in minimal hop. Via simulation results it could be justified that the discussed scheme achieves better filtering capacity and resilience to compromised nodes.*

Keywords: *False data,Filtering,Security,Wsn*

I. INTRODUCTION

A wireless sensor network is a group of specialized sensors with a communication infrastructure for monitoring and regarding conditions at diverse locations. Sum of the commonly monitored parameters are temperatures, humidity, pressure, wind direction, speed, illumination intensity, vibration intensity power line voltage, chemical concentrations vital body condition and so on. The sensors which are deployed to monitored the parameters are equipped with wireless interfaces with which taken communicate to one another to form a network. The design of such network depends significantly on the applications and it must consider factors such as environments, the application's design objectives, cost hardware and system constrain. Sensor nodes have battery limitations security threats, shorter lifespan and few more characteristics which are active research topics. In WSN, sensor nodes obtain measurements from the physical components process the measurements and send data to the controller through networks, According to the sent data, the controller estimates the state of physical system and sends feed backs comments to activators to control the operation of physical systems.[6]. WSN may operate in hostile environment and the sensor nodes in WSN lack tamper –resistance, hardware which increases the chance of being compromised by advisories [7]. For example, the adversaries can use wireless devises to connect to the network and compromise or physically capture sensor nodes through ford injection attacks [8] or node replication attack [9] in which a number of compromise nodes can be controlled by the advisories. The adversaries can inject false measurement reports into the controller through compromise nodes cause the controller to estimates wrong system states and pose dangerous threat to the system. The false reports consume many network computational resources and shorten the life time of the network. Hence, to ensure the normal operation of the system, it is critical to filter injected false data at intermediate notes before arriving to the controller. Generally speaking, en-route filtering is a scheme by which intermediate nodes confirm the authenticity of messages and filter them when those messages travel through the network. Most of the existing en-route filtering schemes are based on authentication, i.e., a legitimate measurement report must carry at least valid message authentication codes (MACs) generated by different valid sensor nodes in WSN, where is the threshold and predefined before WSN is deployed. En-route Filtering is an energy efficient scheme as the false messages are filtered at intermediate nodes before posing the impact on remaining nodes in the network.

II. RELATED WORKS

To defend against false data-injection attacks an investigation on the protection-based defense and detection-based defense is made. For the protection-based defense, we identified and protected critical sensor and make the system more resilient to attacks The steady state Kalman filter is used to perform state estimation

while a failure detector is employed to detect anomalies in the system. An attacker wishes to compromise the integrity of the state estimator by hijacking a subset of sensors and sending altered readings.

EXISTING SCHEMES	REMARK	DRAW BACKS
SEF [5]	Uses MAC for validating data . 70% efficient	Compromised nodes pretend to be legitimate nodes.
IHA [6]	Authentication at every hop	Only filter after T (integer) nodes are compromised.
LBRS [7], LEDS [8] and CCEF[9]	Vulnerable to node failure and denial-of-service attacks.	Excess delay to receive data and system operation is unstable
DEFS [10] and GRSEF [11]	Low resilience to attacked nodes . DEFS introduces lots of extra control messages.	Incur the consumption of energy resources on nodes.

Table1. Comparison of prevailing schemes

III. SYSTEM MODEL

3.1Background

Generally speaking, en-route filtering is a scheme by which intermediate nodes confirm the authenticity of messages and filter them when those messages travel through the network. Most of the existing en-route filtering schemes are based on authentication, i.e., a legitimate measurement report must carry at least valid message authentication codes (MACs) generated by different valid sensor nodes in network, where 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 valid MACs. If not, the report is considered a false one forged by the adversary and then dropped. Otherwise, the report is forwarded to the next forwarding nodes along the route.

3.2 Network and Threat Models

There are two types of nodes in the system: sensing nodes and forwarding nodes, shown as green nodes and red nodes in Fig. 3.1. These two types of nodes are denoted as sensor nodes in the paper. Note that the two nodes in Fig. 1 connected with bidirectional link means that these two nodes are within each other's wireless communication range and can 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 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 the adversary. We assume that the adversary can compromise sensor nodes, including both sensing nodes and forwarding nodes. Once a node is compromised, the secret information stored in the node becomes visible to the adversary. The adversary can inject false measurement reports to the controller through compromised nodes. This causes the controller to estimate wrong system states and sends wrong control commands to actuators, posing dangerous threat to the system. The false reports also consume network and computation resources and shorten the lifetime of CPNS. We assume that the controller is well protected and the adversary can only obtain the authentication information through compromising sensor nodes. We also assume that there is a reliable node

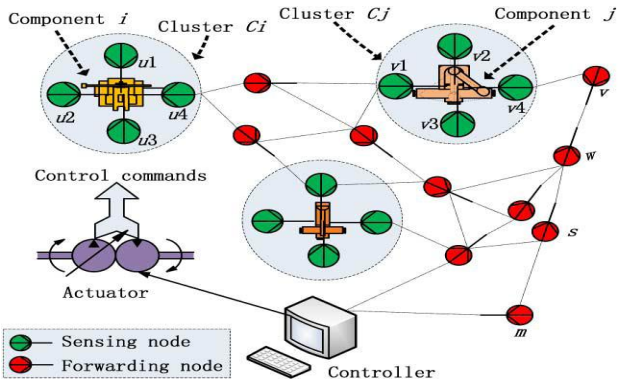

Fig.1 System model

IV. AUTHENTICATION AND SECURITY CONCEPTS

Discussed idea consists of the following two key components

(i) Authentication phase is used to assign the key, local ID of sensing nodes and (ii) Data security phase is used to detect and filter the false measurement reports. These two components will be described in the next two subsections.

4.1 Authentication Phase

Before the sensor nodes are deployed, there is need to prepare a master key and a global primitive polynomial pool. The master key can be generated and stored in the memory of nodes before nodes are deployed and used to produce the cluster key for each cluster. The global primitive polynomial pool consists of several ternary polynomials, which are randomly created before nodes are deployed. The global primitive polynomial pool is used to assign the primitive polynomial to each cluster and its size is $l\left(l < \frac{Ns}{n}\right)$, where n is the number of sensing nodes monitoring a component, Ns is the total sensing nodes in the system. Each monitored component is monitored by n sensing nodes organized as a cluster. It can deploy n sensing nodes close to the monitored component. Those nodes communicate with each other and each node only stores the node IDs of other n-1 sensing nodes in its cluster regardless of the number of hops a node and its neighboring nodes in the cluster. Note that the node does not store the node ID of neighbors outside its cluster even if the neighbors are only one-hop away. The node ID is stored in the node before being deployed In this stage, the network designer initializes all nodes and the network with the parameters such as Kc is the master key(x,y,z) is the element from a set of primitive polynomials, T is the threshold, and H(.) is the hash function, and x,y,z are unknown parameters of the ternary polynomial. The sets of x,y,z represents all sensing node IDs, all forwarding nodes IDs, and all measurement reports of monitored components, respectively. For each sensing node u, the designer stores the master key Kc.Assuming that the controller is well protected and the adversary cannot compromise it, and thus the cluster IDs of all clusters, the masker keys of all clusters, the cluster key generation function can be stored in the controller without losing confidentiality. Hence, the controller can obtain the cluster keys of all clusters. The unreliable wireless communication, the cluster-head may not receive the response messages from the same cluster nodes. If this occurs, the cluster-head considers that these local IDs have not been assigned to cluster nodes. If the cluster-head finds that a local ID has not been assigned, it repeats the above process and assigns the local ID to a node. This process is only used to ensure that each cluster node is assigned one local ID. By screening the local ID attached in the sensing report of monitored components, our scheme can detect the false measurement reports sent by the compromised cluster-header and increase the resilience to false data injection attacks.

4.2 Data Security Phase

To ensure the warning message reaches the first intermediate node before it forwards the report to the next intermediate node should wait a few clock cycles for receiving the warning messages after receiving measurement reports. When the first intermediate node receives the measurement report, it waits for several clock cycles for receiving the warning message. If clock cycles are complete and no warning message arrives, the first intermediate node detects and forwards the measurement report. The number of clock cycles can be pre-defined and the waiting time ensures that the sensing nodes can complete the decision and send out the warning message. In this way, PCREF can drop the false measurement report forged by the compromised cluster-header effectively at the first intermediate node along the forwarding route. 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.By leveraging the polynomial-based message authentication conducts the en-route filtering on false measurement reported from the compromised nodes while the existing approaches cannot do so. The measurement report is 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 the corresponding check polynomial, determines whether the received measurement report $R$is false through validating the following conditions: (i) Condition 1: The Ti as timestamp attached in R is fresh. (ii) Condition 2: T MAPs attached in the report are different and are generated by the sensing nodes in the corresponding cluster, where cluster ID is claimed in the report. (iii) Condition 3: T MAPs can be verified by the corresponding check polynomial stored in the intermediate node.If the above three conditions are not satisfied, the inter-mediate node will drop the measurement report. Otherwise, the measurement report will be forwarded. The timestamp denoted as Ti 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 Ti is timestamp to determine the freshness of the forwarded measurement reports and detect the replayed false report.After receiving the measurement report, the controller validates it in the same way as the intermediate node. Because the controller stores all primitive polynomials and all cluster keys and master keys of all cluster, it can validate all received measurement reports and filter the false measurement reports, which bypass the detection of intermediate nodes. If the report is confirmed as legitimate, the controller decrypts the measurements from the report, and estimates the state of monitored component and sends the commands to the actuators to control the operation of physical systems. Because it contains the complete authentication information, the controller is the last defense in the system and can detect and filter all the false measurement reports forged by the adversary.

4.3 Algorithm

Step1 Cluster formation –Cluster i, Cluster j...

Cluster head election based on energy distance.Cluster members are given unique id by the cluster head

Step2 Master key Kc is decided by the designer and erased after individual cluster key is formed as Kci=f(Kc|CHi)

Step3 Sensing nodes sense data and from each cluster node broadcast it to the corresponding cluster head which aggregate and send to the forwarder node.

Step4 Forwarder node waits for few clock cycles

Case 1: Due to broadcasting nature when cluster head of a cluster broadcast to the next node the nodes in that particular could eavesdrop the node id by which any false id can be intimated.

Step5 When no intimation is made then the forwarded node check the authentication of the data

Case 2 If the data is found illegitimate then it is dropped at the forwarder node and the id of the compromised node is made transparent to other nodes in the network .

Case3 Ch is compromised. The forwarder node waits for a few clock cycle after receiving R.Due to broadcast nature the sensor nodes in cluster eavesdrop report sent from CH to intermediate node if the ID is not match they sent warning signal to forwarder node

Step6 Intermediate node verifies

- Time stamp
- Cluster id
- Node id
- Hash of the report value

Step 7 Forwarder node broadcast the report the controller and it also verify same as the intermediate node and find the false data .If data is found authentic then it is decrypted to know the state of the system

Encryption and decryption

We assume that the input block is given in two w-bit registers A and B. We also assume that key expansion has already been performed, so that the arrays(0, t-1) has been computed. Here figure 2 illustrates the Fiestal structure which is basic principle of the symmetric data security process. Basic operation of RC5 encryption algorithm IS discussed here.

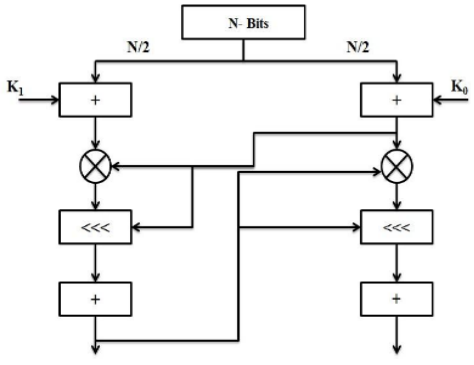

Fig.2 Encryption modules

Mixing in the secret key

The third process is to mix in the user's secret key in the array S and L array.

i=j=0; A=B=0;

Do 3*max(t,c) times;

A=S[i]=(S[i]+A+B)<<< 3;

B=L[i]=(L[i]+A+B)<<< (A+B);
i= (i+1)mod (t);
j= (j+1)mod (c);

V. RESULTS AND DISCUSSIONS

To verify the characteristics and the quality of proposed method variety of simulations are carried out. For better performance analyzes, here we carried out exhaustive test bench simulation. The design is scripted as a verilogHDL file and synthesized using QUARTUS II 9.0 v. The design is synthesized into Cyclone device.

Measurement report	Area (LE's)	Speed(MHz)	Power dissipiation(mW)
Dropped at forward node	464	369.69	117.30
Dropped at cluster	529	452.49	117.29
For successful transmission	464	369.69	117.53

Table 2.Authentication Synthesis Report By Altera Cyclone III Family

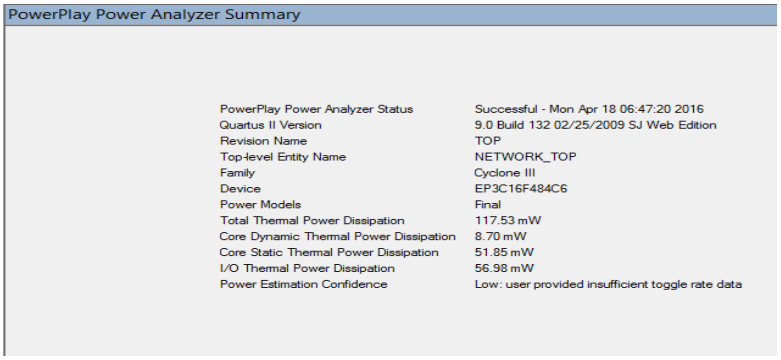

Fig.3 Power model

Here both node ID and cluster ID's values are stored as a text file. The text file is accessed by the Modelsim ALTERA and the corresponding authentication and check polynomials are calculated. These values are then fed to the each and every node which returns the polynomial sequence. The simulated results to validate the efficiency of the algorithm are shown.

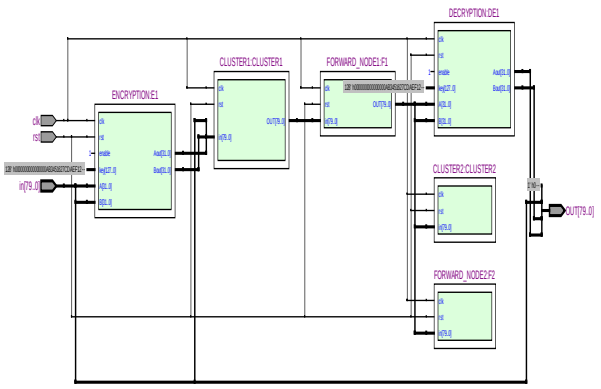

Fig.4 RTL view

The below shown result depict the case in which the forwarder node identified the false data from the compromised node in the cluster 1 before broadcasting to the controller and the packet is dropped at the forwarder node. Hence the possibility to transmit a false report to controller is detected through which the computational resources are kept intact.

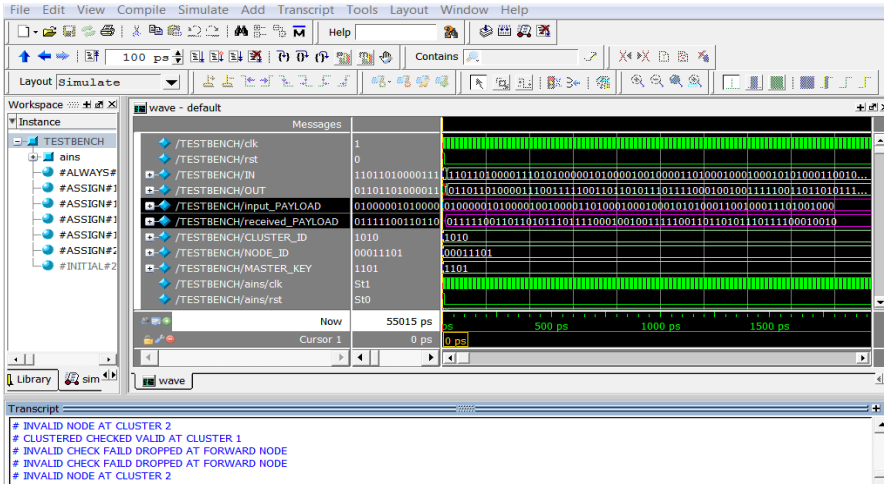

Fig.5 Case 2 of the proposed scheme

VI. CONCLUSION

The false reports consume many network and computation resources and shorten the lifetime of sensor networks. Hence, to ensure the normal operation of the system, it is critical to filter false data at forwarding nodes before arriving at the controller. This scheme could be summarized as a stratagem which can filter false data en-route effectively and achieve high resilience to the number of compromised nodes without relying on static routes and node localization. It adopts hash of the data for endorsing measurement reports to improve resilience to node impersonating attacks. Also it limits the effect of compromised nodes to a small area.

REFERENCES

[1]. F. Wu, Y. Kao, and Y. Tseng, "From wireless sensor networks towards cyber physical systems," Pervasive Mobile Comput., vol. 7, no. 4, pp. 397–413, Aug. 2011.
[2]. A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in Proc. 1st Int. Workshop CyberPhys. Syst. (WCPS), 2008, pp. 495–500.
[3]. M. Pajic, A. Chernoguzov, and R. Mangharam, "Robust architectures for embedded wireless network control and actuations," Trans. Embedded Comput. Syst., vol. 11, no. 4, article no. 82, Dec. 2012.
[4]. A. Albur and A. G. Exposito, Power System State Estimation: Theory and Implementation. Boca Raton, FL: CRC Press, Mar. 2004.
[5]. H. Chan and A. Perrig, "Security and privacy in sensor networks," Computer, vol. 36, no. 10, pp. 103–105, 2003.
[6]. Y. Younan, P. Philippaerts, F. Piessens, W. Joosen, S. Lachmund, and T. Walter, "Filter-resistant code injection on arm," in Proc. 16th ACM Conf. Comput. Commun. Security (CCS), 2009, pp. 11–20.
[7]. K. Xing and X. Cheng, "From time domain to space domain: Detecting replica attacks in mobile ad hoc networks," in Proc. 29th Conf. Inf. Commun. (INFOCOM), 2010, pp. 1595–1603.
[8]. Q. Yang, J. Yang, W. Yu, N. Zhang, and W. Zhao, "On a hierarchical false data injection attack on power system state estimation," in Proc. IEEE Global Telecommun. Conf. (GLOBECOM'11), 2011, pp. 1–6.
[9]. Y. Liu, M. K. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," in Proc. 16th ACM Conf. Comput. Commun. Security (CCS), 2009, pp. 21–32.
[10]. Y. Mo and B. Sinopoli, "False data injection attacks in control systems," in Proc. Preprints 1st Workshop Secure Control Syst., CPS Week, 2010.
[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]. (2010). CPS Week [Online]. Available: http://www.cpsweek2010.se/
[13]. Cyber Physical Networks(CPN) Research Lab. [Online]. Available: http://cpn.berkeley.edu/.