FALSE DATA INJECTION ATTACKS IN CYBER PHYSICAL NETWORK SYSTEM

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

Abstract : Wireless sensor networks (WSN) are expected to interact with the physical world at an unprecedented level to enable various new applications. However, a large-scale sensor network may be situated in a probably unpropitious or even hostile surroundings and potential threats can range from coincidental node failures to intended deface. Due to their relatively small sizes and disregarded operations, sensor nodes have a high risk of being encapsulated and compromised. False sensing reports can be injected through compromised nodes, which could conduct to not only false alarms but also the consumption of limited energy resource in a battery powered network.

I. Introduction

In Cyber-Physical Network Systems (CPNS), attackers could inject false measurements to the controller through compromised sensor nodes, which not just threaten the security of the system, additionally consumes system resources. To deal with this issue, various en-route filtering have been intended for wireless sensor networks. However, these schemes either need flexibility to the quantity of compromised nodes or rely on upon the statically arranged routes and node limitation, which are not suitable for CPNS.

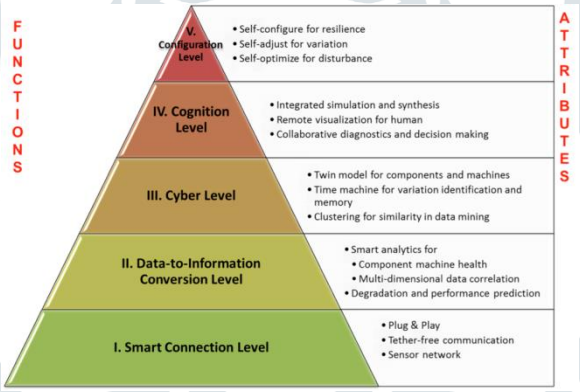

Fig 1 - Cyber physical network system

The false data insertion in a cyber physical network system can be overcome by the formation of clusters where the neighbor sensor node with exactly similar properties will be standardized into the form of clusters. In the hierarchical network structure each cluster has a leader, which is called cluster head (CH). The sensor nodes repeatedly transmit their data to the CH nodes. CH nodes compound the data and transmit them to the base station (BS). CH nodes transmit the data either directly or through the intermediate data transmission with other CH nodes. The BS is the data processing module for the data which is received from the sensor nodes. The Base Station is not variable it's fixed at a place in a stable manner which is up to a point from the all the sensor nodes. The function of each CH is to fulfill ordinary or common functions for all the nodes in each cluster, like collecting all the data before sending towards the BS. In other way, the CH is the sink node for the cluster nodes, and the BS is the sink for the CHs [1].

A cyber-physical system (CPS) is a mechanism that is controlled or monitored by computer-based algorithms, tightly integrated with the Internet and its users. In cyber-physical network systems, physical and software elements are extremely twisted, each working on inconsistent structural and secular scales [2]. The advantages of cluster based environment are: 1) Supporting network extensibility and decreasing energy consumption through data collection. 2) It can localize the route setup within the cluster and thus reduce the size of the routing table stored at the individual node.

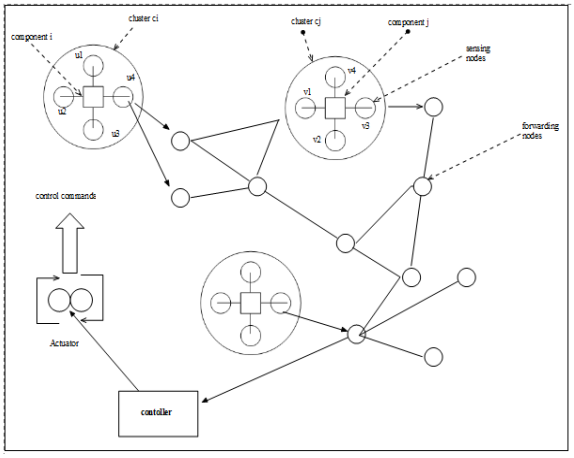

Fig 2 - Mechanism of Cyber physical network system

The main characteristics included in clustering are: Number of clusters, Nodes and CH mobility, Nodes, types and roles, Cluster formation methodology, Cluster-head selection. A long ago number of scheme have been offered for filtering false data in wireless sensor networks where the data is passed from an environment where the sensor nodes are separated. In this report, we have proposed about the compromise resilient en-route filtering scheme where the sensor nodes are organized into the form of clusters, and the data is transferred to Base station (sink) by using forwarding nodes which is act as an intermediate node between the cluster and the base station [3].

II. Proposed system

The proposed system is Polynomial-based Compromised En-route Filtering scheme (PCREF) for wireless network(WSN), which could filter false inserted data successfully and reach a high flexibility to the number of compromised nodes which doesn't depends on the static data dissemination routes and node localization. Preliminary a) The Basics of 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 way which is from source to the sink by using intermediate nodes present in the network [4].

Introducing an approach called Polynomial-based Compromised-Resilient En-route Filtering scheme (PCREF) for CPNS, which could filter false injected data effectively and achieve a high resilience to the number of compromised nodes which doesn't depends on the static data dissemination routes and node localization. PCREF is more suitable for CPNS to monitor and affect mobile physical components and systems. PCREF adopts polynomials instead of MACs (message authentication codes) to verify reports, and can mitigate node impersonating attacks against legitimate nodes. In these, the sharing the authentication information between nodes with a pre-defined probability avoids the node association to share authentication information between source nodes and forwarding nodes, and thus these scheme does not depend on static routes. Monitoring and controlling physical systems through geographically distributed sensors and actuators have become an important task in numerous environment and infrastructure applications. A Novel En-route Filtering against False Data Injection Against in Cyber-Physical Network technologies and new development in cyber-physical networked systems (CPNS). CPNS, consisting of sensor nodes, actuators, controller, and wireless networks, have been widely used to monitor and affect local and remote physical environments. CPNS can make on how we interact with the physical world [5].

The role of intermediate node is not only checks the correctness of the data also it can filter the false inserted data effectively. The intermediate nodes after receiving all the report checks whether it contain valid T-MAC. The report with less number of threshold massage authentication code (T-MAC) will be dropped. If some time any false data is not filtered by the intermediate nodes will be detected by the sink where it gets filtered. In this case the sink which is acts as the final safeguard that holds false reports not filtered out by forwarding nodes. b) Security Model of En-route Filtering: A large sensor network field where nodes are deployed, after the network initialization phase the sensor nodes forms into groups and elect a cluster head based on different parameters like remaining energy, bandwidth and maximum connectivity etc. Whenever any malicious activity found, all the cluster members near to the clusters will sense the movements and report to their cluster heads. After receiving the reports cluster head collect them and sends a single copy of the valid report to the base station through the selected report forwarding nodes.

The selections of report forwarding nodes are up to the central routing protocol's work. And also the selection parameters are independent of the application. There are attackers present in the network are capable of monitoring the communication pattern between the sensor members and the cluster head to guess the message from the reports if intercepted. In this each cluster contains at most t-1 compromised nodes, which may collaborate with each other to generate false reports by sharing their secret key information. The potential attack which we mentioned in this dissertation is DoS attacks. DoS attacks include selective forwarding and report disrupt. In cyber physical Networks the nodes are typically DoS attacks. DoS attacks include selective forwarding and report disrupt. In cyber physical Networks the nodes are typically autonomous and self-interested and may belong to different establishment. If they well established to generate efficient data sharing mechanism, the nodes also have different hardware and energy capabilities and may pursue different goals. Here is the plan for

energy conservation, the mobile nodes are battery driven and one of the major sources of energy consumption is radio transmission, selfish nodes are unwilling to lose their battery energy in relaying other users' packets [6].

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 [7].

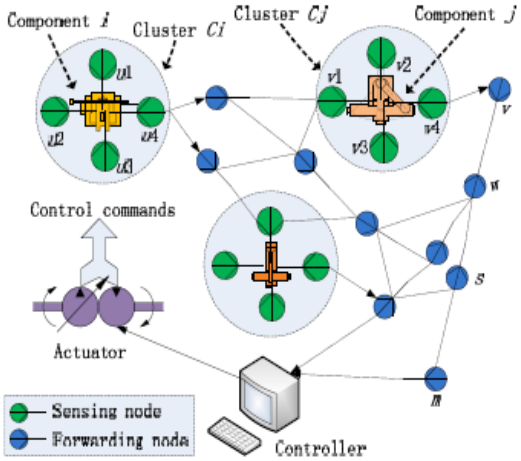

Fig 3 - System Architecture

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.

CPNS may operate in hostile environments and sensor nodes in CPNS lacking tamper resistance hardware increases the possibility to be compromised by attackers. The attacker can inject false measurement reports to the controller through the compromised nodes. This causes the controller to estimate wrong system states and poses the dangerous threats to the system [8].

III. RESULTS AND DISCUSSION

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

- Packet delivery ratio
- Delay
- 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.

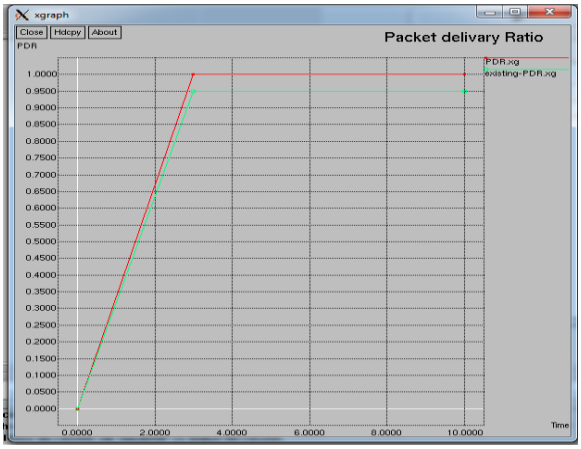

Fig 4 - Analyzing Delivery Ratio

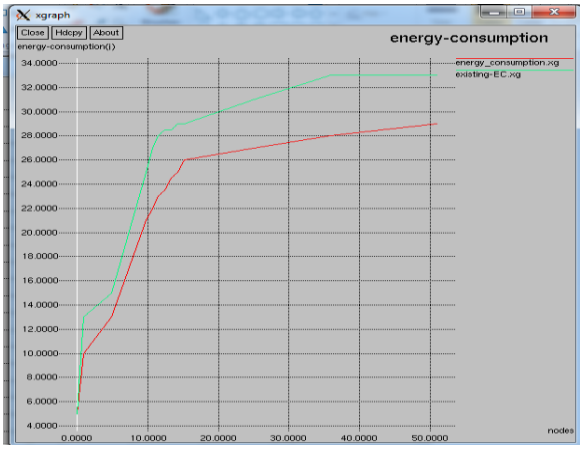

Fig 5 - Comparing Energy Consumption In Existing system

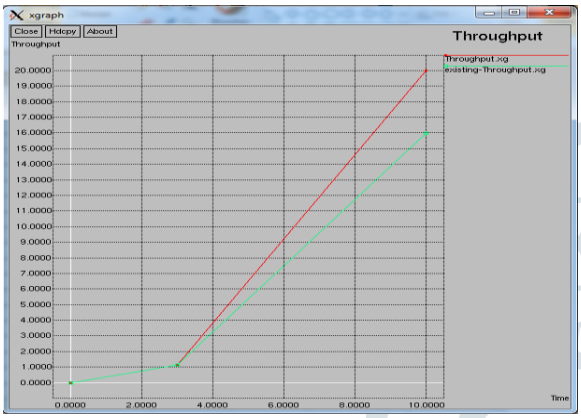

Fig 6 - Comparing Delay In Existing system

Fig 4 indicates the packet delivery ratio (PDR) is the total number of packets received by the destination nodes to the total number of packets sent by the source nodes. Where x-axis derives number of nodes and y-axis derives the packets delivered. Store and forward policy in both the system proposed a good delivery ratio. Co-operative nature of nodes proposed works efficiently in internetwork. The multicast scenario in proposed system not only encourages node to cooperate but also establishes a relation and competitiveness between them. Also charge and reward function adds some improvements in accessing the data circulation process. It successfully leads us to the objective achievements.

Fig 6 indicates average Delay is the time taken for a message to reach the subscribers from the publisher. Here in above graph x-axis denotes number of nodes and y-axis denotes delay in milliseconds. The encryption mechanism can be developed to get cut down the delay time in proposed system but due to security purpose minute delay will be considered. As military and governance purposes we required top level of security. So we can deal with minute delay rather than breach of information. Fig 5 shows energy consumption is the ratio of total number of messages relayed over the total number of unique messages delivered. Here in graph below x-axis depicts number of nodes and y-axis denotes the overhead ratio i.e. data packets arrived at subscribers end.

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 handles authentication information and separates the incorrect results measurement. PCREF receives polynomials for supporting estimation reports to enhance versatility to the node impersonating attacks.

IV. 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.