International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 5 512 - 515

An Efficient Polynomial-based Filtering Against False Data Injection Attack in CPNS

Ms. Sanjana R. Heralgi
Department of Computer Engineering
D. Y. Patil College of Engineering, Akurdi
Savitribai Phule Pune University, Pune, India
Email: sanjana.heralgi@gmail.com

Ms. D. B. Gothawal
Department of Computer Engineering
D. Y. Patil College of Engineering, Akurdi
Savitribai Phule Pune University, Pune, India
Email: dgohil.1519@gmail.com

***Abstract*—** Cyber Physical Network System (CPNS) is gaining lot of attention in many applications like, transportation networks, vehicular networks, life-critical applications and many more. Hence, the system needs to be protected from various kinds of attacks that degrade the system's performance. There are many different types of attacks that are possible on cyber physical systems, among them false data injection attack is a serious threat to the system's security. In this type of attack, the adversary compromises sensor nodes, inject false data and send them to the controller through compromised nodes. This makes the controller to estimate wrong system states which leads to various serious issues. Therefore, the false data must be filtered out before it reaches the sink. If all the false data flow towards the controller then it will be bottle neck to filter all the false data and this could paralyze the network. To resolve this issue many filtering schemes have been developed in the past, all use Message Authentication Codes (MACs) for report endorsement and en-route filtering. But they are not suitable for CPNS because of static routes and lack resilience to the number of compromised nodes. Hence, an enhanced scheme has been proposed which uses polynomials instead of MAC for report endorsement and also uses bloom filtering along with en-route filtering. Hence, this achieves high resilience to the number of compromised nodes and achieves high filtering efficiency.

Keywords **-** *Wireless Sensor Networks, Cyber Physical Network System, False Data Injection Attack, En-route Filtering, Polynomials, Bloom Filtering.*

*****

I. INTRODUCTION

As there is rapid advancement in electromechanical systems and wireless technologies the Cyber Physical Systems (CPS) demands greater attention in wide variety of applications. It has been considered as quotidian in many research areas. The CPS system is used in many application areas such as Transportation network, vehicular networks, aerial vehicles, healthcare applications, safety-critical systems, military surveillance and many more [1].

The CPS systems are the systems that connect the physical world with the world of communication and computation [2]. Cyber-Physical Systems are the integrations of computation with physical processes [3] with the use of sensors and actuators. CPS are the systems that bridge the world of computation and communication (cyber world) with the physical world
[2]. The operations of the CPS systems can be monitored, controlled, coordinated and integrated by communication and computation.

CPS provides the interconnection for human to human, human to machine and machine to machine interaction [4] through the wireless network connectivity and user control on the actuation side [5].

Cyber Physical Networked System (CPNS) consists of sensors, actuators, controllers and wireless networks. The sensors in CPNS are used to estimate the state of the physical system. The sensor nodes are manually deployed around the physical component that is to be monitored. The state of the physical component is continuously monitored by the sensor nodes and the measurement report will be sent to the controller through the wireless networks [1]. The controller acknowledges the actuator about the state of the component, the actuator then sends the feedback commands to the controller to take necessary actions [1].

Due to the size and cost constraints, the sensor nodes lack in tamper resistance hardware which makes them vulnerable to various kinds of attacks, such as sybil attacks, node impersonation attacks, selective forwarding, wormholes, Denial of service (DoS) attack [6][7][8]. In addition to these attacks, there is another attack called false data injection attack [9] that thwarts the security of the system. As many systems are safet critical, any successful attack can lead to economic loses and obstruct the functionality of the system[9].

There are two classes of attack that thwart the security of the cyber physical system: Denial of Service (DoS) attack and false data injection (deception) attack [9]. Detection of false data injection attack is more difficult than DoS attack, because the DoS attack only prevents the exchange of information but false data injection attack affects data integrity by modifying the original packets [11].

The false data injection attack is called as an insider attack [10]. It not only make the controller receive incorrect measurement reports so that it should take wrong decisions but it also take significant energy of the sensor nodes. In this attack, the adversary first compromises several sensor nodes and access all the keying materials stored in them. It then uses these keying materials and act as legitimate node. Once it knows the secret keys it then can induce fake measurement reports to the controller. If all the false reports flow towards the controller, the energy of the sensor nodes wasted in addition the controller becomes the bottle neck to filter all the false data and the network could get paralyzed quickly.

Therefore, the false data must be filtered before it reaches the controller. To filter the false data early the en-route filtering mechanisms have been used by many schemes. In en-route filtering, each and every intermediate node performs the report verification. If the report is said to be from the

unauthenticated node, the report will be dropped otherwise it will be forwarded towards the controller.

Many en-route filtering have been developed so far against the false data injection attack and all of them use Message Authentication Code (MAC) for report endorsement. In addition all previous mechanisms lack in resilience to the number of compromised nodes and depend on static routes and node localization, which is not suitable for cyber physical networked systems. Hence, an enhanced polynomial- based filtering scheme against false data injection attack has been developed to achieve better filtering efficiency. Our system uses polynomial instead of MAC for report endorsement and also uses bloom filtering.

Bloom filtering is a space efficient data structure used to test the group membership in a space efficient way [12]. It filter out an element that is not a in the set [13]. The two main advantages of Bloom filtering technique are: (i) they use less memory and (ii) have fast query time. There are two modes of operation in bloom filters: element insertion and membership query.

The remainder of the paper is organized as follows: in section II the schemes that are built against false data injection attack have been discussed. In section III the enhanced polynomial-based filtering scheme have been proposed. In section IV the results are discussions are given. Section V is the conclusion and future scope.

II. RELATED WORK

To mitigate the impact of false data injection attack many filtering mechanisms have been developed so far. All the schemes use message authentication code for report endorsement. Some of the filtering schemes have been briefly discussed in the following paragraphs.

Fan Ye et al. proposed Statistical En-route Filtering (SEF) [14] that first conducted en-route filtering. In SEF each report must be is validated by multiple MACs. Each node along the route to the sink verifies the correctness of MAC. If false data escapes the verification then sink will serve as final goal keeper to filter the false data. The keys are derived from global key pool. But if the intermediate nodes itself are compromised then SEF cannot detect the compromised nodes.

Zhu et al. proposed Interleaved Hop-by-Hop Authentication (IHA) [15] scheme. Every node in the network has two associations, one with lower node and other with upper node called lower and upper association respectively. The report is forwarded only if it is successfully verified by lower association node. The report is transmitted in an interleaved hop by hop fashion. This also has threshold limitation and hop by hop transmission may chafe the network.

LBRS [16] and LEDS [17] are the location-based en-route filtering scheme. These two technique avoid threshold limitation that was encountered in previous technique by adopting location-based key generation technique. LEDS also provides end-to-end data security. But the location-based keys require node localization and static routes which are not suitable for CPNS.

Yang et al. proposed Commutative Cipher-based En-route Filtering (CCEF) [18] in which a secure connection is established in a region between the sink node and cluster head based on commutative cipher. CCEF filters out false data early by en-route filtering. The intermediate node verifies the session authentication based on a probability, therefore it is difficult to adjust the changing ratio of false traffic.

STEF [19] is a secure ticket-based en-route filtering in which every node in the network is assigned a ticket by the sink node. Every report generated by the sensor nodes is carries tickets, the report is transmitted further only if it carries valid ticket. But for the cluster head there is only one way communication for the traversal of the ticket downstream.

The GRSEF [20] is a Grouping-based Statistical En-route Filtering. It is an enhancement to the SEF mechanism, in which the sensor nodes are divided into groups and one among them is selected as a group master. The group master is responsible for collecting all the reports from the group members and transmit the report to the sink. It filters false data in early stage but has low resilience if more nodes are compromised.

Zhen yu et al. proposed Dynamic En-route Filtering (DEFS)[21], it has capability to adapt to dynamic network. This scheme prevents both denial of service attack and false data injection attack. For report endorsement each node has a chain of hashed authentication keys. It uses hill climbing approach for key dissemination. However, have low resilience and incurs extra control messages.

III. PROPOSED WORK

To mitigate the impact of false data injection attack an efficient filtering scheme has been proposed that overcomes the limitations of previous filtering approaches. This scheme uses polynomials instead of MAC for report endorsement and also uses bloom filtering to improve the performance.

A. Assumptions

The assumptions are as follows. The sensor nodes are deployed manually near the physical component to be monitored. There are two types of polynomials assigned to every node, authentication polynomial and check polynomial. The nodes within the cluster stores the authentication polynomial of its own and check polynomial of the its cluster head. The cluster head stores the check polynomial of other cluster head.

The sensor nodes continuously monitor the physical component and sends report regarding state of the system at fixed time intervals. When a report is generated by the sensor node, it must be verified by its neighboring sensor nodes and the report is forwarded to the cluster head. The cluster head verifies the authenticity of the report by en-route and bloom filtering if it is valid then report is sent to the controller else it is dropped by the cluster head. It ensures that the fake measurement does not reach the controller and male it to estimate wrong system state and take wrong action.

B. Problem Definition

Detecting and filtering false data that are injected by the adversary is the focus of this scheme. The false data can be filtered at very early stages by en-route filtering. But en-route filtering requires pair wise key establishment which make the adversary easy to capture the secret keys. Also sometimes the false data may escape the en-route filtering.

The bloom filtering scheme is used to check the membership of the node. If the node wants to transmit some

message to the controller, its membership is checked first. If it is not a member of the set than it is not allowed to send the report. The bloom filtering is used to reduce the key size and also used for packet recovery.

C. System Architecture

Figure 1 shows the system architecture of the proposed scheme. The sensor nodes are organized into clusters, each cluster is having a cluster head. The sensing nodes are placed near the physical component to be monitored. There are two types of sensor nodes: sensing nodes and forwarding nodes. The sensing node can monitor, sense and forward the report to the controller, whereas the forwarding node can only forward the report.

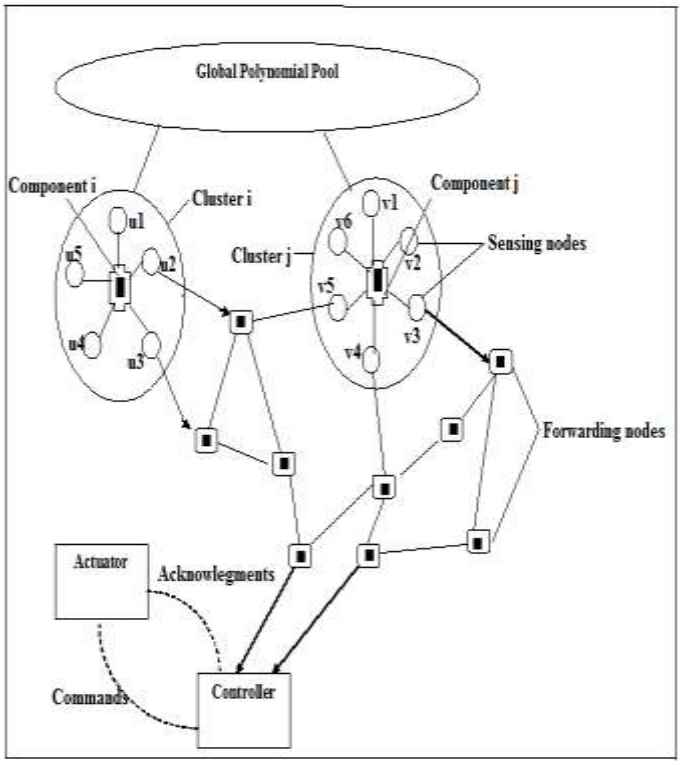

Figure 1. System Architecture

For each node a unique polynomial is assigned. There are two types of polynomial authentication polynomial and check polynomial. Authentication polynomials are assigned to the sensing nodes and check polynomials are assigned to forwarding nodes. Sensing nodes continuously monitor the component and sends the measurement report to the controller. Nodes generate Message Authentication Polynomial (MAP) whenever a report is generated. Each sensing node that detected the same event attaches its MAP to the report and sends measurement report to the forwarding node. The report is verified by all the intermediate node. If the forwarding node finds that the report is fake it drops the report and does not forward it further. If the report is valid then it is forwarded to the controller. Controller then estimates the state of the physical system and takes corresponding actions.

D. Enhanced Polynomial-based Filtering

Algorithm 1 Polynomial-based bloom filtering

Input: Sensing nodes $\{S_1, S_2 \ldots S_n\}$, Forwarding nodes $\{F_1, F_2, \ldots F_n\}$, reports $\{r_1, r_2, \ldots r_n\}$
Output: Authenticated reports $\{r_1, r_2, \ldots r_n\}$
1. All the nodes in the network are initialized
Kc, f(a, b, c), T, H(.)
2. Authentication polynomial of node x
auth(x) = α f(x, b, c), where = $2, 2^2, 2^3, 2^4$
4.Check polynomial of node x
verf(x) = β f(x, a, c), where = $2^5, 2^6, 2^7, 2^8$
5. Reports $r_1, r_2, \ldots r_n$
are generated by
Report r = $((E)_{K_{Ci}}$ — x — MAP)
6. MAP is generated by each sensing nodes by
MAP = $auth_x$(b, c) = αf(x, b, H($(E)_{K_{Ci}}$))
7. Report along with MAP are sent to forwarding node.
8. Forwarding node performs en-route filtering and forwards report only if following conditions are satisfied.
Condition 1: The time stamp *Time* attached to the report must be fresh.
Condition 2: T MAPs attached in the report should be different and generated by the sensing nodes.
Condition 3: T MAPs can be verified by the intermediate node using stored check polynomial.
9. Controller performs filtering same as forwarding node.
10. If report is valid, it decrypts and send to actuator.
11. Bloom filtering is performed by the cluster head and the controller.
12. Membership of nodes are checked each time the nodes forward report to the controller.
13. For 'n' sensor nodes it has 'h' hash functions.
14. Marks '1' if particular sensor node is present, else '0'.

This scheme uses polynomials for report endorsement and also uses bloom filtering along with en-route filtering. The main reason behind using bloom filtering is its space efficiency in memory constrained sensor nodes. Sometimes the false report may escape from en-route filtering and reaches the destination. Therefore, the bloom filtering is also used to check membership query, if particular sensor node does not belong to the set then it cannot send the report further.

IV. RESULTS

As the sensors in the CPNS are used to monitor the state of the physical system. To implement the scenario of cyber physical network system we have taken three physical attributes viz., lifts, camera and battery status of the PC. The measurement reports are continuously sent to the controller through the cluster head. Every report must go through the cluster head, the cluster head will only forward the valid measurement to the controller. If the report is found to be false then it is discarded and it is not sent to the controller. Bloom filtering also provides packet recovery i.e., as the false data are not sent to the controller particular measurement report will be missing. Therefore, the true report will be recovered by bloom filtering approach.

TABLE I. COMPARISON OF PCREF AND ENHANCED POLYNOMIAL BASED FILTERING IN TERMS OF REPORTS.

Parameters Measured	Existing System	Proposed System
No. of reports sent	100	100
No. of reports dropped	18	25
No. of reports received by Controller	82	75
No. of reports recovered	-	25

The above table I shows the comparison of the existing system and proposed system in terms of number of reports sent from the source including false reports. The number of reports considered is 100, and if 25 are false report among them, then in existing system cannot filter all the false reports some may escape from the filtering. In the proposed system almost all the false reports are dropped and not sent to the controller. It also shows the number of packets recovered that is it can recover the original report that was not sent because of false reports. Figure 2 shows the comparison graphically.

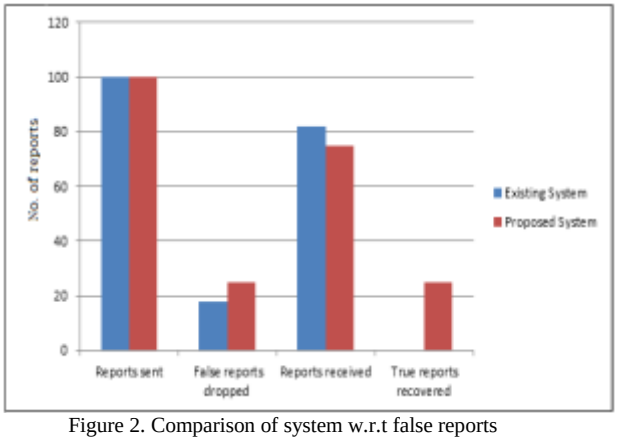

Figure 2. Comparison of system w.r.t false reports

V. CONCLUSION

The false data injection attack is a serious menace to the cyber physical network system. Adversary can compromise sensor nodes in CPNS and inject false measurements in to the controller. This thwarts the security of the system and also consumes lot of network resources. To deal with this issue many filtering schemes have been proposed. But most of them have some limitations and are not suitable for CPNS. Hence, enhanced polynomial-based filtering scheme has been proposed that uses en-route filtering and bloom filtering, which can filter false data effectively and efficiently and have high resilience to the number of compromised nodes. Bloom filtering does not support removal of elements from the set. In addition to this, bloom filtering produces more false positive reports by query operation. Hence, cuckoo filter can be used, which has insertion as well as deletion operation.

ACKNOWLEDGMENT

We are thankful to all the authorities of IJRITCC for providing a platform to present our work. We express our deepest gratitude to the college authorities for technical guidance and infrastructure. Lastly we wish to thank the researchers and reviewers for their contributions because of which we could complete this work.

REFERENCES

[1] Yang, Xinyu, et al. ”A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems.” Computers, IEEE Transactions on 64.1 (2015): 4-18.
[2] Rajkumar, Ragunathan Raj, et al. ”Cyber-physical systems: the next computing revolution.” Proceedings of the 47th Design Automation Conference. ACM, 2010.
[3] Lee, Edward A. ”Cyber physical systems: Design challenges.” Object Oriented Real-Time Distributed Computing (ISORC), 2008 11th IEEE International Symposium on. IEEE, 2008.
[4] Ali, Salman, et al. ”Network Challenges for Cyber Physical Systems with Tiny Wireless Devices: A Case Study on Reliable Pipeline Condition Monitoring.” Sensors 15.4 (2015): 7172-7205.
[5] Shi, Jianhua, et al. ”A survey of cyber-physical systems.” Wireless Communications and Signal Processing (WCSP), 2011 International Conference on. IEEE, 2011.
[6] Lu, Rongxing, et al. ”BECAN: a bandwidth-efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks.” Parallel and Distributed Systems, IEEE Transactions on 23.1 (2012): 32-43.
[7] Venkatraman, K., J. Vijay Daniel, and G. Murugaboopathi. ”Various attacks in wireless sensor network: survey.” International Journal of Soft Computing and Engineering 3.1 (2013).
[8] Padmavathi, Dr G., and Mrs Shanmugapriya. ”A survey of attacks, security mechanisms and challenges in wireless sensor networks.” arXiv preprint arXiv:0909.0576 (2009).
[9] Cardenas, Alvaro A., Saurabh Amin, and Shankar Sastry. ”Secure control: Towards survivable cyber-physical systems.” The 28th International Conference on Distributed Computing Systems Workshops. IEEE, 2008.
[10] Wang, Eric Ke, et al. ”Security issues and challenges for cyber physical system.” Proceedings of the 2010 IEEE/ACM Int’l Conference on Green Computing and Communications & Int’l Conference on Cyber, Physical and Social Computing. IEEE Computer Society, 2010.
[11] Mo, Yilin, et al. ”False data injection attacks against state estimation in wireless sensor networks.” Decision and Control (CDC), 2010 49th IEEE Conference on. IEEE, 2010.
[12] Nojima, Ryo, and Youki Kadobayashi. ”Cryptographically Secure Bloom-Filters.” Transactions on Data Privacy 2.2 (2009): 131-139.
[13] Hebden, Peter, and Adrian R. Pearce. ”Data-centric routing using Bloom filters in wireless sensor networks.” Fourth International Conference on Intelligent Sensing and Information Processing (ICISIP-06), IEEE Press, Bangalore, India. 2006.
[14] Ye, Fan, et al. ”Statistical en-route filtering of injected false data in sensor networks.” Selected Areas in Communications, IEEE Journal on 23.4 (2005): 839-850.
[15] Zhu, Sencun, et al. ”An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks.” Security and privacy, 2004. Proceedings. 2004 IEEE symposium on. IEEE, 2004.
[16] Yang, Hao, et al. ”Toward resilient security in wireless sensor networks.” Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing. ACM, 2005.
[17] Ren, Kui, Wenjing Lou, and Yanchao Zhang. ”LEDS: Providing location-aware end-to-end data security in wireless sensor networks.” Mobile Computing, IEEE Transactions on 7.5 (2008): 585-598.
[18] Yang, Hao, and Songwu Lu. ”Commutative cipher based en-route filtering in wireless sensor networks.” Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th. Vol. 2. IEEE, 2004.
[19] Kraub, Christoph, et al. ”STEF: A secure ticket-based en-route filtering scheme for wireless sensor networks.” Availability, reliability and security 2007. ARES 2007. The second international conference on. IEEE, 2007.
[20] Yu, Lei, and Jianzhong Li. ”Grouping-based resilient statistical en-route filtering for sensor networks.” INFOCOM 2009, IEEE. IEEE, 2009.
[21] Yu, Zhen, and Yong Guan. ”A dynamic en-route filtering scheme for data reporting in wireless sensor networks.” IEEE/ACM Transactions on Networking (ToN) 18.1 (2010): 150-163.