Hop by Hop Authentication Scheme using ECDSA for WSN

D. Nishan Nithya*, S. Gomathi
Department of CSE, Francis Xavier Engineering College, Tirunelveli
***Corresponding author: E-Mail: nithymurthy@gmail.com**

ABSTRACT

In Cyber-Physical Networked Systems (CPNS), mugger could inject false computation to the controller through compose sensor nodes. This not only abuses the security of the system, but also affected the total network system. To deal with this problem, a number of En-Circuit Filtering arrangements have been created for wireless sensor networks. However, these arrangements either lack of volition to the number of compose nodes or depend on the idiotically arranged routes and node localization, which are not suitable for CPNS. In this paper, a Polynomial-Based Compromised-Rebounding En-circuit Filtering scheme (PCREF) is proposed, which can strain false infuse data and achieve a high volition to the number of compose nodes without depend on idiotically routes and node localization. Particularly, PCREF adopts polynomials rather of MACs (Message Authentication Codes) to confirm measurement reports to achieve the volition attacks. Each node stores two types of polynomials. They are authentication polynomial and check polynomial derived from the vital polynomial. PCREF performed better filtering capacity and faces many volition to the broad number of compose nodes in comparison to the existing schemes.

KEY WORDS: Cyber Physical Networked system, false measurement report, sensor networks, Polynomial-Based En-Route Filtering (PCREF), HbHAMAC (Hop by Hop Anonyms Message Authentication Code).

1. INTRODUCTION

Check and controlling physical systems are the significant tasks in large applications. In CPNS new development schemes consist of sensor nodes, actuators, controllers, and wireless networks. In CPNS, the main assignment are hit the physical components, processing the analysis. Through the grill, the hit data will be sent to the controller. The controller will analyse the level of physical system and send reply to the actuators. It is troublesome to strain the false injected data to ahead nodes, before the controller scope. There are many schemes designed to filter the false injected data such as SEF (Staidly En-Route Filtering), LBRS (Light Weight and Compromise-Rebounding Message Authentication Scheme), DOS (Denial of Service), Grouping –based Rebounding Staidly En-Route Filtrate for Sensor Networks (GBSEF). These suggestion have their control and it will not effectively conception with mugger. Polynomial Based Compromise Rebounding En-Route Filtering Scheme (PCREF) for CPNS. The PCREF can strain the false infuse data wrongly and perform a high volition to the number of composed nodes, without act on static data and knob localization. This arrangements consists of two types. They are sensor nodes and forwarded nodes. The Sensing node will forward the analysis report along with the route. Each and every knob supplies two types of polynomials. They are authentication polynomial and analysis polynomial. The Suspect node treasures the authentication polynomial of individual cluster. To strain the false data injected by raider using Hop by Hop Anonymous Missive Authentication Code Scheme effectively. A MAC requires two inputs. That is missive and a secret key. The grantee is to verify the message and message's sender has shared the secret key. The litter value would then be different when the sender does not know the private key. There are four types of MACs. They are; a) unconditionally secure, b) hash work-based, c) flow cipher-based and d) block cipher-based. Authentication is a functioning in which the documentation provided are correlated to those on file in a database of endorsement users' information.

Hop-by-hop transport is used to control the leakage of data in network. In Hop-by-Hop transport, block of data are tolerate from node to node in a fountain-and-forward presence. HbHAMAC (Hop by Hop Anonymous Missive authentication Code) is designed based on Asymmetrical Curve that can provide the limitless source and that are invisibility. An qualified Hop by Hop Missive Authentication mechanism is used for WSNs without the gate limitation. This theorem is used for securing the message against attackers.

Polynomial Based Compromise Rebounding En-Route Filtering Scheme (PCREF) algorithm is proposed to strain the false interject data defectively. It will achieve high violation to the number of composed nodes without depend on static nodes and node localization.

Related Works: Chen and Lei (2010), proposed "Filtering fake messages en-circuit in wireless multi-hop networks," The authors used Bloom filter techniques to build an authentication plain, which is called En-Circuit Authentication Bitmap (EAB). EAB helped nodes on the routing direction to filter out fake data in high success rate, thus bound the injection attacks within the one or two hops from the match. Low estimation cost and Low communication overhanging are the advantages of this work. It cannot be used to deal with attacks related to Cyber Physical cycle Systems.

Prema, and Saravanan (2009), proposed Efficient KCC Telecast Authentication Scheme in WSNs. The authors used Koblitz Curve Telecast Authentication scheme using signature authenticate for WSNs. This scheme employed only one KCCDSA (Koblitz Curves Cryptography Data Processor Signature Algorithm) signature to

authenticate all transmission messages. The upper of the signature is amazed over all transmission messages. It provided trivial in terms of computation, communication and storage overhead. It can bring out immediate authentication that a receiver authenticates a transmission message upon receiving it are advantages. The heavy overhanging occurred when the number of telecast messages increases.

Nithya Menon and Praveena (2009), proposed BECAN: A Bandwidth Efficient Combining Authentication Scheme for Wireless Sensor Networks. A Bandwidth-Energetic Combining Authentication (BECAN) scheme is used for filtering an injected fake data in Wireless sensor Networks. To filter the false data, the BECAN scheme supported Combining Neighbor Router (CNR)-based filtering mechanism. It resisted the observed forgeries and High filtering choice these all are the advantages. It must need further development to reduce the gang injecting false data attack from mobile agree sensor nodes.

Pajic (2012), proposed Robust Building for Embedded Wireless Network Control and Actuations. The authors used Embedded Virtual Machine (EVM). EVM approach is used for a program thinking where the controller is responsible for controlling and timing. It is possible to compute task assignment efficiently. Less scrabbled is one of the main drawbacks.

Lee (2005), proposed A design to Control the choice of try to Verify a Report in Statistical En-Circuit Filtering. The Authors used Statistical En-Route Filtrate of Injected Fake Data in Sensor Networks (SEF) techniques are used as a insurance technique about the fake data injection push. SEF can verify that whether a detail is false report or not through the en route filtering. This can reduce energy consumption to verify detail is the advantage. Some nodes which consume energy too much cannot filter out the false detail efficiently, these all are disadvantages.

Xinyu Yang (2008), proposed A Novel En-Circuit Filtering Scheme against Fake Data Injection raid in Cybe. Physical Networked Systems. The authors used Polynomial Based Compromise-Rebounding En-route Filtering Scheme (PCREF) technique is used for strain fake data effortful and achieve a high difficult to the number of composed nodes without depend on fixed routes and knob localization.

2. PROPOSED DETECTION SCHEME

Hop by Hop asymmetric curve digital designation algorithm is designed based on asymmetric curves which provided limitless source that are invisibility. An efficient Hop-by-hop Missive Authentication mechanism is used for WSNs without any gate Limitation. An powerful key management framework is proposed to ensure idle of the compromised nodes. An authentication scheme is formed to achieve the following goals such as Message Authentication, Message Incorrectness, Hop by Hop message authentication, Integrity and Location Privacy, node compromise toughness, and to increase efficiency. Message authentication is direct solutions to unauthorize of abused missive from being expressed with WSN. Because of this reason, many authentication schemes are proposed to incorruption verification intended for Wireless Sensor Network (WSNs). These schemes can largely be branched in two categories. They are public-key centered approaches and symmetric-key centered approaches.

Authentication generation theorem: Expect that q is a message to be transmitted. The private key of the message sender z is dt, $1 \leq t_i \leq o$. To generate an efficient HbHAMAC for message m.

z performs the ensuing three steps: Select a random and pair wise different k i(j) for each $1 \leq i \leq n-1$, $i \neq t_i$, and compute i from (i , z) = k_i

- Choose a random ki ∈ Zp and compute rt from (rt, yt) = ktG − ∑ i≠t rihiQi such that rt ≠ 0 and $s_t \neq s_i$ for any j ≠ q, where hi l ←− h (m, s_i).
- Compute s = kt + ∑ i≠t k_i + stdtmt mod N. The HbHAMAC of the missive m is defined as:

H(m) = (m, H, s1, y1, · · · , rn, zn, H).

Verification of HbHAMAC algorithm: For z to verify an HbHAMAC (m, H, r1, y1, · · ·, rn, yn, h), it must have a copy of the public keys Q1, · · ·, Qn. Then it:

- Checks that $p_i \neq O$, j = 1, · · · , n, otherwise it is invalid
- Checks that p_j , k = 1, · · · , n lies on the curve
- Checks that $np_k = O$, k = 1, · · ·, n

After that, z follows these steps:

- Verify that s_i, p_i, k= 1, · · ·, n, and s are integers in [1, N − 1]. If not, the signature is invalid.
- Calculate hi l ←− h(k, s_i), where h is the same function used in the signature generation.
- Calculate (x_i, y_i) = hE − ∑n_i=1.
- The signature is valid if the first coordinate of ∑ i (s_i, y_i) equals x_o, otherwise it is invalid.

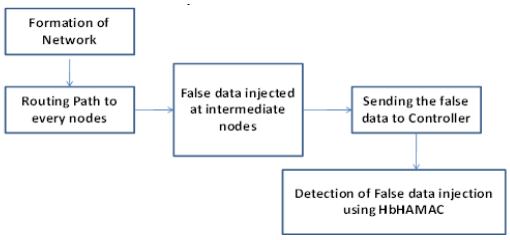

Figure.1. System Architecture

In Fig.1, describes the formation of network there is many routing path to each and every nodes. In that routing path many fake data can inject at any intermediate nodes. Now send the false data to the controller. The Controller will disclose the location of fake data injection by attack node using HbHMAC.

System Modules:

Basic routing module: Basic broadness module is used to create a number of knob and to assign which node is sender and which node is receiver also to create the routing direction between the nodes.

Include hacking in basic routing module: Include tease in basic broadness module which included an attacker node in routing path. The data hacked between the routing nodes and the attacker will inject the fake to during the data transmission. Then the modified data will be sending to the next hop knob and finally the fake data is reached at destination.

Misbehavior broadcast Authentication: Misbehavior broadcast Authentication is used to provide authentication arrangement for nodes to avoid the hackers' injected traffic. This arrangement is used to avoid the traffic injected by hackers and reduce packet fall during the packet transmission and this broadcast is used to detect the attacker's node.

Secure Acknowledgement: Secure Acknowledgement is used to provide the security to dealer and target nodes. This security process to avoid the tease process and restricted the attacker also this module chooses the alternative routing path when the attackers were involved in routing.

Performance Analysis:

Throughput: Throughput is used to amplitude the total rate of data emitted over the network, including the rate of data set from CHs to the sink and the rate of data set from the nodes to their CHs.

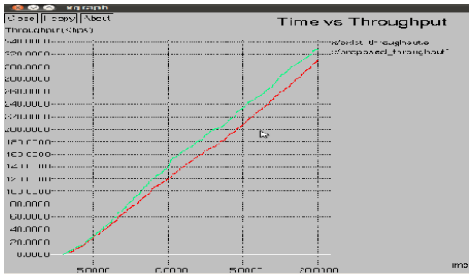

Figure.2. Throughput

Packet Trace Ratio: Packet Trace Ratio is used to amplitude the strength of protocol and is determined by dividing the total number of dropped packets by the total number of spread packets.

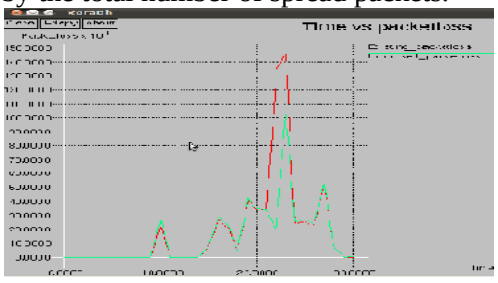

Figure.3. Packet Trace Ratio

Delay: Delay of a network specifies how long it takes for a part of data to transit across the network from one node to another node. It is typically measured in multiples or division of seconds.

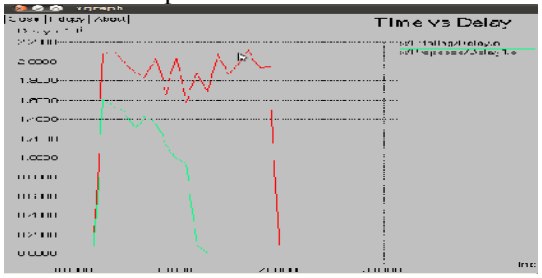

Figure.4. Delay

Overhead: Overhead is any aggregate of excess or indirect estimation time, memory, high frequency, or other resources that are required to complete a particular goal.

3. EXPERIMENTAL RESULT

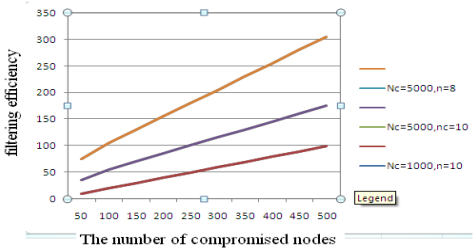

Figure.5. Filter Efficiency Vs Number of Compromised Nodes

Fig.5, Represents the number of agree nodes Vs Filter Efficiency. The number of agree nodes is plotted along x-axis and filtering efficiency is plotted along y-axis. Nc5000, n=8 has increased at level of 300 in filter efficiency. PCREF has maintained the high confidentiality of a component with the increased number of composed nodes. The number of composed nods decreases when the confidentiality toughness of PCREF.

4. CONCLUSION

Polynomial based Compromise Rebounding En-circuit Filtering Scheme (PCREF), which can filter fake data en-circuit effectively and achieved High resolve to the number of agree nodes without depend on fixed routes and knob localization. Our developed schemes achieved better strain capacity and flexibility to a large number of agree nodes.

REFERENCES

Albrecht M, Gentry C, Halevi S and Katz J, Attacking cryptographic schemes based on perturbation polynomials, In Proc. of the ACM CCS, 2009.

Chen X, Makki K, Yen K and Pissinou N, Sensor network security, A survey, IEEE Communications Surveys and Tutorials, 11 (2), 2009, 52–73.

Chen Y.S and Lei C.L, Filtering false messages en-route in wireless multi-hop networks, In Proc. of IEEE WCNC, 2010.

Chen Y.S and Lei C.L, Filtering false messages en-route in wireless multi-hop networks, in proc. IEEE Wireless Commun. Netw. Conf. (WCNC), 2010, 1-6.

Lee H.W, Moon S.Y and Cho T.H, Statistical En-Route Filtering of Injected False Data in Sensor Networks (SEF), IEEE j. sel. Areas Commun., 23 (4), 2005, 839-850.

Liu Y, Reiter M.K and Ning P, False data injection attacks against state estimation in electric power grids, In Proc. of the 16th ACM conference on Computer and communications security, 2009.

Nithya Menon, Praveena S, BECAN Bandwidth-Efficient Cooperative Authentication (BECAN) scheme, in proc. 27th IEEE Int. Conf. Comput. Commun. (INFOCOM), 2009, 1418-1428.

Pajic M, Chernoguzov A and Mangharam R, Robust architectures for embedded wireless network control and actuations, Trans. Embedded Comput. Syst, 11 (4), 2012, 82.

Prema P, Saravanan P, Efficient KCC Broadcast Authentication Scheme in WSNs, in proc 27th IEEE Int Conf Comput., 2009, 1419-1429.

Ren K, Lou W and Zhang Y, Leds, Providing location-aware end-to end data security in wireless sensor networks, IEEE Transactions on In Mobile Computing (TMC), 7 (5), 2008, 585–598.

Subramanian N, Yang C and Zhang W, Securing distributed data storage and retrieval in sensor networks, In Proc. of the 27th IEEE International Conference on Pervasive Computing and Communications (Per Com), 2007.

Yu L and Li J, Grouping –based Resilient Statistical En-Route Filtering for Sensor Networks (GBSEF), in Proc. 28th IEEE Int. Conf. Comput. Commun. (INFOCOM), 2009, 1782-1790.

Zhang W, Subramanian N and Wang G, Light weight and compromise resilient message authentication in sensor networks, in proc. 27th IEEE Int. Conf. Comput. Commun (INFOCOM), 2008, 1418-1426.