International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in; editorijoer@gmail.com

Vol.4., Issue.6., 2016
Nov-Dec.

RESEARCH ARTICLE

ISSN: 2321-7758

HOP BY HOP AUTHENTICATION SCHEME USING MAC FOR WSN

D. NISHAN NITHYA[1], S.GOMATHI[2], P.JENIFER[3]

[1]M.E student, Department of Computer Science, Francis Xavier Engineering College, Tirunelveli, Tamil Nadu, India

[2, 3] Assistant Professor, Department of Computer Science, Francis Xavier Engineering College, Tirunelveli, Tamil Nadu, India

ABSTRACT

In Cyber-Physical Networked Systems (CPNS), mugger could inject false measurements 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-Route Filtering schemes have been created for wireless sensor networks. However, these schemes either lack of toughness to the number of compose nodes or depend on the statically arranged routes and node localization, which are not suitable for CPNS. In this paper, a Polynomial-Based Compromised-Resilient En-route Filtering scheme (PCREF) is proposed, which can filter false injected data and achieve a high toughness to the number of compose nodes without depend on static routes and node localization. Particularly, PCREF adopts polynomials instead of MACs (Message Authentication Codes) to confirm measurement reports to achieve the toughness attacks. Each node stores two types of polynomials. They are authentication polynomial and check polynomial derived from the basic polynomial. PCREF performed better filtering capacity and faces many toughness to the large number of compose nodes in comparison to the existing schemes.

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

I. INTRODUCTION

Monitoring and controlling physical systems are the important tasks in large applications. In CPNS new development schemes consist of sensor nodes, actuators, controllers, and wireless networks. In CPNS, the main tasks are measuring the physical components, processing the measurements. Through the network, the measured data will be sent to the controller. The controller will measure the level of physical system and send reply to the actuators. It is difficult to filter the false injected data to ahead nodes, before the controller reached. There are many schemes designed to filter the false injected data such as SEF (Statically En-Route Filtering), LBRS (Light Weight and Compromise-Resilient Message Authentication Scheme), DOS (Denial of Service), Grouping –based Resilient Statistical En-Route Filtering for Sensor Networks (GBSEF). These schemes have their control and it will not effectively conception with

mugger. Polynomial Based Compromise Resilient En-Route Filtering Scheme (PCREF) for CPNS. The PCREF can filter the false injected data defectively and perform a high toughness to the number of composed nodes, without commit on static data and node localization. This scheme consists of two types. They are sensor nodes and forwarded nodes. The Sensing node will forward the measurement report along with the route. Each and every node supplies two types of polynomials. They are authentication polynomial and check polynomial. The Sensing node stores the authentication polynomial of each cluster. To filter the false data injected by adversary using Hop by Hop Anonymous Message Authentication Code Scheme effectively. A MAC requires two inputs. That is message and a secret key. The receiver is to verify the message and message's sender has shared the secret key. The hash value would then be different when the sender does not know the secret key. There are four types of MACs. They are 1.unconditionally secure, 2.hash work-based, 3.flow cipher-based and 4.block cipher-based. Authentication is a process in which the documentation provided are compared to those on file in a database of endorsement users' information.

Hop-by-hop transport is used to control the flow of data in network. In **Hop-By-Hop** transport, block of data are forwarded from node to node in a store-and-forward manner. HbHAMAC (Hop by Hop Anonymous Message authentication Code) is designed based on Elliptic Curve that can provide the unlimited source and that are invisibility. An Efficient Hop by Hop Message Authentication mechanism is used for WSNs without the threshold limitation. This algorithm is used for securing the message against attackers.

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

II. RELATED WORKS

In [20] Y.-S. Chen and C.-L. Lei, proposed "Filtering false messages en-route in wireless multi-hop networks," The authors used Bloom filter techniques to build an authentication plain, which is called En-Route Authentication Bitmap (EAB). EAB helped nodes on the routing direction to filter out false 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 Networked Systems.

In [2] P.Prema, P.Saravanan proposed "Efficient KCC Broadcast Authentication Scheme in WSNs"The authors used Koblitz Curve Broadcast Authentication scheme using signature authendicate for WSNs. This scheme employed only one KCCDSA (Koblitz Curves Cryptography Digital 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 achieve immediate authentication that a receiver authenticates a transmission message upon receiving it are advantages. The heavy overhanging occurred when the number of broadcast messages increases.

In [16] Nithya Menon, S.Praveena proposed "BECAN: A Bandwidth Efficient Cooperative Authentication Scheme for Wireless Sensor Networks. "A Bandwidth-Energetic Cooperative Authentication (BECAN) scheme is used for filtering an injected false data in Wireless sensor Networks. To filter the false data, the BECAN scheme supported Cooperative 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.

In [4] M. Pajic, A. Chernoguzov, and R. Mangharam, proposed "Robust Architectures for Embedded Wireless Network Control and Actuations. The authors used Embedded Virtual Machine (EVM). EVM Technique is used for a program thinking where the controller is responsible for controlling and timing. It is possible to compute task assignment efficiently. Less scalability is one of the main drawbacks.

In[13] H. W. Lee, S. Y. Moon, and T. H. Cho, proposed "A Method to Control the Probability of Attempts to Verify a Report in Statistical En-Route Filtering, "The Authors used Statistical En-Route Filtrate of Injected False Data in Sensor Networks (SEF) techniques are used as a insurance technique about the false 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.

In[13] Xinyu Yang, Jie Lin, Wei Yu, Paul-marie Moulema, Xinwen Fu, and Wei Zhao, proposed "A Novel En-route Filtering Scheme Against False Data Injection Attacks in Cybe.Physical Networked Systems. The authors used Polynomial Based Compromise-Resilient En-route Filtering Scheme (PCREF) technique is used for filter false data effectively and achieve a high difficult to the number of composed nodes without depend on static routes and node localization.

III. PROPOSED SYSTEM

Hop by Hop Anonymous Message Authentication Code (HbHAMAC) is designed based on elliptic curves which provided unlimited source that are invisibility. An efficient Hop-by-hop Message Authentication mechanism is used for WSNs without any threshold Limitation. An efficient key management framework is proposed to ensure idle of the compromised nodes. An authentication scheme is designed 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 unauthorized of abused messages from being forwarded with wireless sensor Network (WSNs). Because of this reason, many authentication schemes are proposed to incorruption verification intended for Wireless Sensor Network (WSNs). These schemes can largely be divided in two categories. They are public-key centered approaches and symmetric-key centered approaches.

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

z performs the following three steps:

1) Select a random and pair wise different k i(j) for each $1 \le i \le n - 1$, $i \neq t_i$, and compute i from $(i , z) = k_i$
2) Choose a random ki ∈ Zp and compute rt from $(rt, yt) = ktG - \sum j \neq t \; rihiQi$ such that $rt \neq 0$ and $s_t \neq s_i$ for any $j \neq q$, where hi l ←− h (m, s_i).
3) Compute $s = kt + \sum j \neq t \; k_i + stdtmt \bmod N$. The HbHAMAC of the message 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:

1) Checks that $p_j \neq O$, j = 1, · · · , n, otherwise it is invalid
2) Checks that p_j , k = 1, · · · , n lies on the curve
3) Checks that $np_k = O$, k = 1, · · · , n .

After that, z follows these steps: 1) Verify that s_i , p_i , k= 1, · · · , n, and s are integers in [1, N − 1]. If not, the signature is invalid.

2) Calculate hi l ←− h(k, s_i), where h is the same function used in the signature generation.

3) Calculate $(x_i, y_i) = hE - \sum n_i=1$.

4) The signature is valid if the first coordinate of ∑ i (s_i , y_i) equals x_o, otherwise it is invalid.

System Architecture

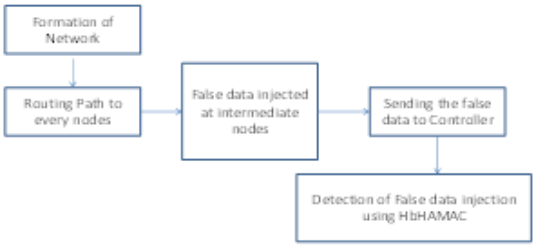

Fig 1: System Architecture

In Fig 1: describes the formation of network there is many routing path to each and every nodes . In that routing path many false data can inject at any intermediate nodes. Now send the false data to the controller. The Controller will

detect the location of false data injection by attack node using HbHMAC.

IV. MODULES

A. Basic routing module: Basic routing module is used to create a number of nodes and to assigned which node is sender and which node is receiver also to create the routing path between the nodes.

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

C. Misbehavior Report Authentication: Misbehavior Report Authentication is used to provide authentication scheme for nodes to avoid the hackers' injected traffic. This scheme is used to avoid the traffic injected by hackers and reduce packet loss during the packet transmission and this module is used to detect the attacker's node.

D. *Secure Acknowledgement:* Secure Acknowledgement is used to provide the security to sender and receiver nodes. This security process to avoid the hacking process and restricted the attacker also this module chooses the alternative routing path when the attackers were involved in routing.

V. PERFORMANCE ANALYSIS

A. *Throughput:* Throughput is used to measures the total rate of data sent over the network, including the rate of data sent from CHs to the sink and the rate of data sent from the nodes to their CHs.

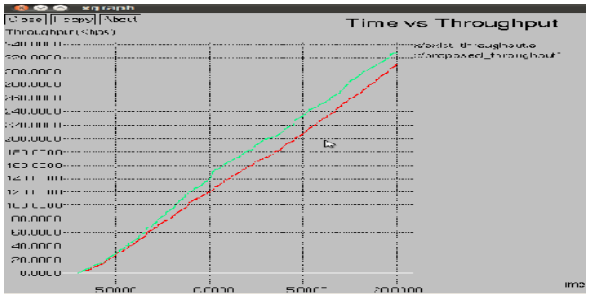

Fig 2: Time Vs Throughput

B. Packet Drop Ratio: Packet Drop Ratio is used to measures the robustness of protocol and is calculated by dividing the total number of dropped packets by the total number of transmitted packets.

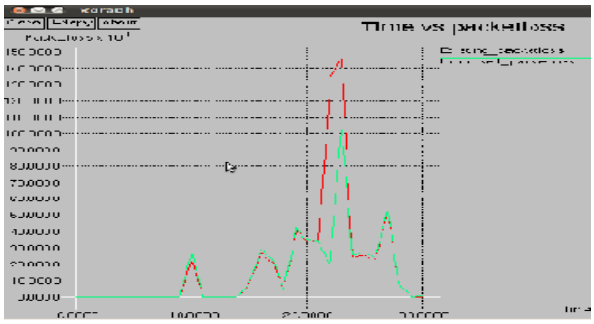

Fig 3:Time Vs Pocket loss

C. *Delay:* Delay of a network specifies how long it takes for a bit of data to travel across the network from one node or endpoint to another. It is typically measured in multiples or fractions of seconds.

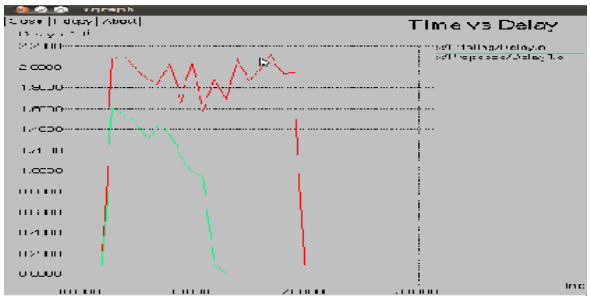

Fig 4: Time Vs Delay

D. *Overhead:* Overhead is any combination of excess or indirect computation time, memory, bandwidth, or other resources that are required to attain a particular goal.

VI. EXPERIMENTAL RESULT

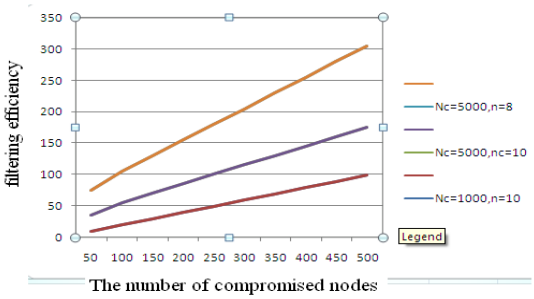

Fig 5: Filter Efficiency Vs Number of Compromised Nodes.

Fig 5 Represents the number of compromised nodes Vs Filter Efficiency. The number of compromised 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.

VII. CONCLUSION AND FUTURE WORK

Polynomial based Compromise Resilient En-Route Filtering Scheme (PCREF), whicsh can filter false data en-route effectively and achieved High toughness to the number of compromised nodes without depend on static routes and node localization. Our developed schemes achieved better filtering capacity and flexibility to a large number of compromised nodes.

In future Elliptic Curve Cryptography (ECC) based digital signature scheme will be used to reduce the computation such as hackers and encrypt the messages. Elliptic Curve, in that curve the messages are hidden. So it is very protective from attackers.

REFERENCES

[1]. Cyber Physical Networks (CPN) Research Lab. http://cpn.berkeley.edu/.

[2]. Northeast Blackout of 2003 http://en.wikipedia.org/wiki/Northeast Blackout of 2003.

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

[4]. A. Albur and A. G. Exposito. Power System State Estimation: Theory and Implementation. CRC Press.

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

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

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

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

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

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

[11]. 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.

[12]. H. W. Lee, S. Y. Moon, and T. H. Cho," Statistical En-Route Filtering of Injected False Data in Sensor Networks (SEF),"IEEE j.sel.Areas Commun vol, 23, no.4, pp. 839-850, Apr. 2005.

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

[14]. P.Prema1, P.Saravanan," Efficient KCC Broadcast Authentication Scheme in WSNs"in proc 27th IEEE Int Conf Comput, 2009, pp.1419-1429.

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

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