International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 03 | Mar 2019 www.irjet.net p-ISSN: 2395-0072

Enhanced ID based Data Aggregation and Detection Against Sybil Attack using Challenge Response Authentication Protocol

S. Syed Nawas Husain[1], Dr. M. Mohamed Sathik[2], Dr. S. Shajun Nisha[3]

[1]M.Phil Research Scholar, PG & Research Department of Computer Science, Sadakathullah Appa College, Tirunelveli, Tamilnadu, India
[2]Principal, Sadakathullah Appa College, Tirunelveli, Tamilnadu, India
[3]Assistant Professor & Head, PG & Research Department of Computer Science, Sadakathullah Appa College, Tirunelveli, Tamilnadu, India

---

Abstract - *In recent year's security of wireless sensor network attracted intensive attention in both research and applications. Many aspect of wireless sensor network applications are defense, industrial process monitoring and control, machine health monitoring, etc. In this paper we presented Challenge Response Authentication protocol (CRAP) between the transaction source to destination, which generates unique key and match the response key to provide unique encrypted communication for every transmission. In the earlier system, coalition attack can be detected through transaction details. Here, we are using Sybil attack, which theft the information of identity nodes while data transmission, The CRAP is used here to prevent such Sybil attacks. The performance of analyzed detection scheme is evaluated using performance detection ratio and provides better result.*

1. INTRODUCTION

Wireless Sensor Network (WSN) has been widely used in military, industrial and medical applications during the last decade. [1] The network is consisted of more of thousands of sensor nodes. Usually the sensor nodes have limited power, memory, and computing abilities, then energy conservation become a very important problem of WSN researches. The cluster based WSN is proposed for this purpose [2].The cluster head (CH) is responsible for the management and data process an aggregation of the cluster member nodes (cluster member, CM). Selective Nodes send their data to the cluster head and the cluster head aggregates cluster head data of all nodes within it and sends data to the Base Station. Clustering process enables bandwidth and can increase system capacity. Of course, it helps improve power control and better of resource allocation.

This system attentive the cluster based on wireless sensor network. Because of the rapid development of WSN, many works have been presented in recent years. They include the authentication field, efficient protocol routing and data fusion algorithms. Also, there are few security related works which we will talk about in this system. Security problems put many applications in the devil of a hole [5]. The attackers could scout the network traffic easily and trace the data information from any sensor node if the privacy such as identity or location is lack of protection. Privacy has become a critical issue for the WSN deployments. For traditional network, anonymous communication is an important method protecting the privacy of users. It includes anonymity node, location privacy node, untraceability and unlinkability. And, it can be split it into three anonymous types which including sender anonymity, recipient anonymity and unlinkability.

Many anonymous protocols have been proposed for the traditional network in last decades. Chaum's mixnet and DCnet are the original work about it. But both approaches require public key cryptosystems and can't be used into WSN due to power and resources constrains of sensor nodes. So it is essential to develop mechanisms that suited for WSN. [3]In this system, we design a sensor anonymity enhancement plan based on pseudonym for clustered WSN. The scheme includes two phases. It can protect the privacy both of the CMs and the CH nodes. [1] We then using entropy based method to evaluate anonymity of the scheme and implement the scheme using NS2 simulator to test the performance of the scheme. Both the theoretical and the empirical study imply that our proposed scheme can provide good anonymity for both CMs and CHs.

1.1. ATTACK FREE NETWORK FORMULATION

A wireless sensor network consists thousands of small nodes which are distributed over the network. These nodes sense the sensitive data from the location and send the sensitive message to the base station.[4] The base station will verify the information and ID which is send by the sensor nodes. These sensor nodes are position in hostile environment and the nodes are unattended many replicas of which makes an adversary to compromise the sensor nodes and make. In robotics advances developing an variety of new architectures for autonomous. In network communications of mobile nodes are useful for network repair and event detection. [2], [4] The mobile nodes are compromised inject the forgery data and disrupt network operations and eavesdrop on network communications. Software based

replica detection plans have proposed for static sensor networks. The nodes sensor also report the location state that identify their positions and send to the base station. In this system, the proposed compromised node detection plan based on the sequential probability ratio test

2. LITERATURE SURVEY

Noor et al. [1] proposed an identity based signature aggregate scheme keeps data integrity with designated verifier this scheme providing more secure and efficient process we make use of Elliptic cryptography curve and Diffie hellman assumption data transmitted compromised aggregators to provide privacy.

Yingying et al. [2] proposed a method for detecting indentity based attack including spoofing and Sybil attacks RSS based methods of identity-oriented authentication and detection problem In robust to detect attacks use of different transmission in various power levels and built real-time localization system.

Pengwenlong Gu et al. [3] proposed to support vector machine based Sybil attack method for improving road safety and driving experience in vehicle driving patterns are mainly represented using Driving paterns matrices begin variation of vehicle and Sybil nodes classify into SVM methods during virtual nodes.

Kamdeo et al. [4]. Harsh operating environment are open of susceptible WSNs can many kinds of attacks has prevented. Here using Sybil.one of the most dangerous attacks in WSNs. here using Sybil attack Detection Algorithm (SDA) for detecting and preventing Sybil attack in WSNs.SDA is more secured for transmission data in any way avoid Sybil attack.

Bin Zeng et al. [5] recommended Ant Colony Optimization (ACO) algorithm using third party initiate between honest node if a malicious node successfully fools be trusting as used to prevent significant protocol ones in this system probability is high accuracy variants be evaluate fake identities with trusted edges.

3. SYSTEM MODEL

3.1. Challenge Response Authentication Protocol:

In Challenge Response Authentication Protocol have three phases. Detection accuracy in which increased when compared to the previous phase Challenge-response mechanisms based on symmetric-key techniques require the claimant and the verifier to share a symmetric key [5]. For closed systems with a small number of users, each pair of users may share a key a priori; in larger systems employing symmetric-key techniques, identification protocols often involve use on-line server trusted in which each party shares a key. The online server effectively acts like the hub of a spoke wheel, providing a common session key to two parties each time one requests authentication.

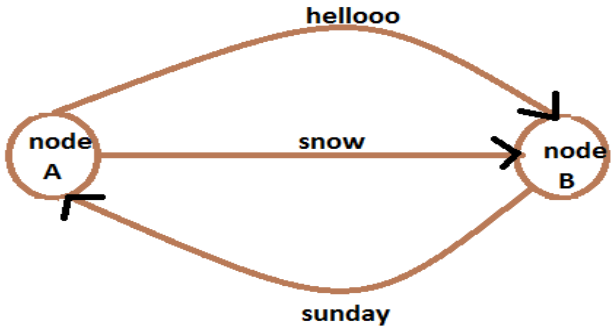

Fig 3.1

Phase 1

- Create a group of mobile nodes, Sybil node,and normal node.
- According to the procedure nodes are taken from base station
- The base station node A sends HELLOOO packets to all the node B and responsible node B sends SUNDAY to node A for topology verification.
- The nodes with minimum packet drop are the chosen as the trust nodes.
- The trust nodes now become the head nodes with a combination of its own member nodes.
- The member nodes send their ID and then power value to the head nodes.
- The head node checks for the nodes with a power value below the threshold value
- Thus the power value is lesser than the threshold value, then the nodes are detected as Sybil nodes.

Phase II

- Two nodes nearest to Sybil nodes are selected as senders n1, n2.
- Two Sybil nodes are selected and the receivers are s1, s2.
- Packets are sent to n1 and n2 to both receivers
- Since both identities are present at the same node, there is collision of packets leading into the packet drops.
- The distance between the receivers is found.
- The are nodes suffers from Sybil attack
- If the nodes are very close and then process.

Phase III

- If there occur a hop between the Sybil identities, then the nodes are not Sybil nodes.

- If no hops, then the nodes are confirmed to be above the attack and they will be removed from the network two nodes closer to Sybil nodes are selected as sender's n1 and n2.
- Two Sybil nodes hop between the Sybil identities and then the nodes are not Sybil nodes has been detection.
- If no hops, then the nodes are confirmed to be under attack and then they process will be removed from the network

4. OUTLINE OF PROPOSED WORK

- The nodes were formed in WSN.
- There were three types of nodes: Source Node, Static Node and Mobile Node[4].
- Each node were assigned with ID for aggregation network traffic data.
- CRAP technique implemented for analyzing node identity.
- Sybil Attack Detection through Genetic Algorithm.
- Performance can be evaluated through PDR, Energy Efficient, Attack Detection Ratio, etc.

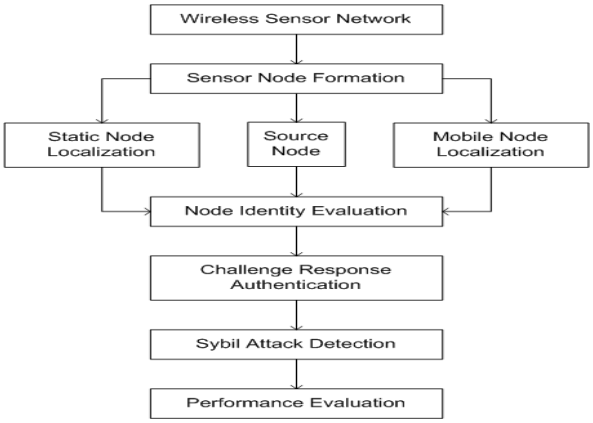

Fig 4.1

5. Result

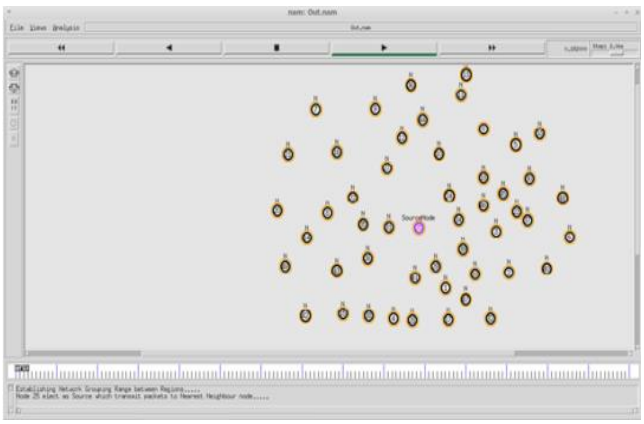

Fig 5.1

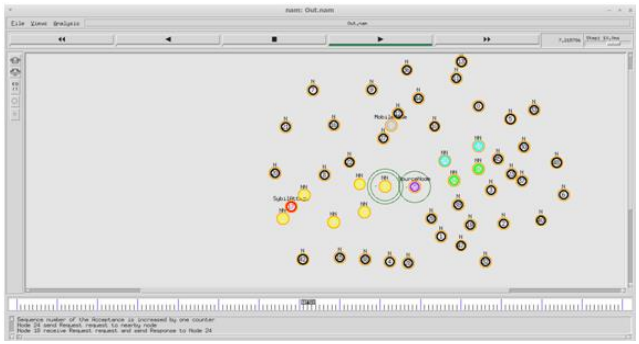

Fig 5.2

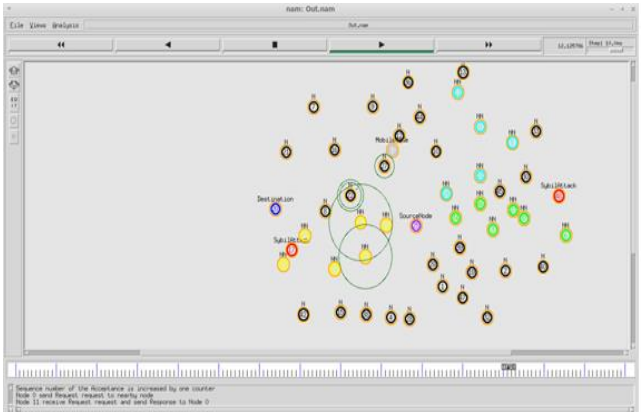

Fig 5.3

Graph Representation

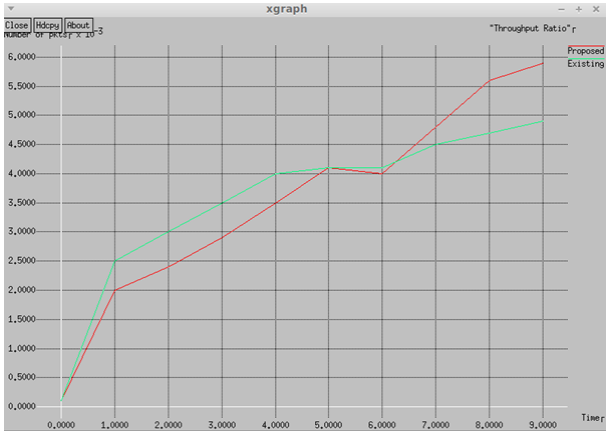

Fig 5.4 (Attack Detection Ratio)

6. CONCLUSION

This system concludes that the malicious nodes in wireless sensor networks are detected by using a new statistical testing technique called sequential probability ratio testing. Using this technique the compromised sensor nodes are detected efficiently in mobile sensor networks. Our work has

focused on the privacy problem of cluster based on wireless sensor network and using anonymous method to protect the privacy of the nodes. We designed a novel sensor anonymity enhancement scheme for WSN. In order to prove the efficacy of the scheme, we used entropy based method to evaluate the degree of anonymity our scheme achieved. For all the above mentioned strategies demonstrates that our scheme can protect the privacies of both the sensor nodes and the cluster heads, and can use in any cluster based on wireless sensor network

7. FUTURE SCOPE

The proposed system is done on the evaluation parameters, in scheme of proposed able to identify and Sybil attack in those networks and very efficiently. Also the mitigation scheme works effectively. The experimental results show that works better in terms of good detection rate, low false positive rate and low false negative rate. The future scope of this work may include making scheme more cost efficient and easy to implement in any type of network. The main focus will be on detection rate and false positive rate.

REFERENCES

1. Noor Basha, Kavya N, Manjushree K, Arogyasheela A and Bhavana T, " ID-Based Aggregate Signature Scheme for Wireless Sensor Networks Using Secure and Efficient Data Transmission ", International Research Journal of Computer Science (IRJCS), Issue 05, Volume 4 (May 2017)

2. Yingying Chen, Yang, Wade Tappe and Richard P.Martin, " Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks ", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 59, NO. 5, JUNE 2010.

3. Pengwenlong Gu, Rida Khatoun, Youcef Begriche and Ahmed Serhrouchni, " Support Vector Machine (SVM) Based Sybil Attack Detection in Vehicular Networks ",IEEE Wireless Communications and Networking Conference (WCNC),2017.

4. Kamdeo Prasad and Chandrakant Mallick," A Mobile Agent based Sybil Attack Detection Algorithm for Wireless Sensor Network", in International Conference on Emergent Trends in Computing and Communication (ETCC 2015)

5. Bin Zeng and Benyue Chen, " SybilACO: Ant colony optimization in defending against Sybil attacks in the wireless sensor network ", International Conference On Computer and Communication Technologies in Agriculture Engineering, 2010(IEEE)

6. T. N. Manjunatha, M.D. Sushma, K.M. Shivakumar, "Sybil Attack Detection Through On Demand Distance Vector Based Algorithm" In Wireless Sensor Networks, Issue June 2013(JIARM).

7. R. Amuthavalli, Dr. R. S. Bhuvaneswaran, "Detection and Prevention of Sybil Attack In Wireless Sensor Network Employing Random Password Comparison Method ", Issue September 2014(JTAIT).

8. S.Sharmila and G Umamaheswari, "Detection Of Sybil Attack In Mobile Wireless Sensor Networks", Issue MarApr 2012(IJESAT).

9. D.Sheela, V.R.Srividhya, Amrithavarshini and J.Jayashubha, "A Mobile Agent Based Security System of Wireless Sensor Networks against Cloning and Sink Hole Attacks", Issues ICCTAI'2012.

10. Rupinder Singh Brar and Harneet Arora," Mobile Agent Security issue in Wireless Sensor Networks ", Issue 1, January 2013(IJARCSSE).

11. James Newsome, Elaine Shi, Dawn Song and Adrian Perrig," The Sybil Attack in Sensor Networks: Analysis & Defenses", Issue 27 April 2004(IPSN).

12. Karen Hsu, Man-Kit Leung and Brian Su, "Security Analysis on Defenses against Sybil Attacks in Wireless Sensor Networks", Issue 2008(IEEE).

13. Manjunatha T. N, Sushma M. D, Shivakumar K. M, " Security Concepts and Sybil Attack Detection in Wireless Sensor Networks" in international journal of emerging trends and technology in computer science April 2013.

BIOGRAPHIES

S. Syed Nawas Husain received the B.sc degree in Computer Science from MS University in 2016 and M.sc degree in Computer Science from MS University in 2018.He is currently pursuing the M.phil degree in Computer Science. Her research interest mainly include domain of Network Security.

"Dr. M. Mohamed Sathik M.Tech., M.Phil., M.Sc., M.B.A., M.S., Ph.D has so far guided more than 35 research scholars. He has published more than 100 papers in International Journals and also two books. He is a member of curriculum development committee of various universities and autonomous colleges of Tamil Nadu. His specializations are VRML, Image Processing and Sensor Networks.

Dr. .S.Shajun Nisha Assistant Prof & Head of PG and Research Department Of Computer Science, Sadakathullah Appa College. She has completed M.Phil. (Computer Science) and M.Tech (Computer and Information Technology) in Manonmaniam Sundaranar University, Tirunelveli. She has completed her phd in .She has involved in various academic activities. She has attended so many national and international seminars, conferences and presented numerous research papers. She is a member of ISTE and IEANG and her specialization is Image Mining.