International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 08, August-2015

Sensor Anonymity Enhancement and Duplicate Node Detection Scheme for Clustered Wireless Sensor Network

Divya K. V.
PG Student, Department of ECE
Sree Narayana Gurukulam College Of Engineering
Kadayirippu, Kerala, India

Shiji Abraham
Assistant Professor, Department Of ECE
Sree Narayana Gurukulam College Of Engineering
Kadayirippu, Kerala, India

***Abstract*— The continued advancements in micro-electronic-mechanical-systems, wireless technologies and smart sensors enabled the deployment of wireless sensor network (WSN) in large amounts in communication applications. Hostile environments of operation in real time make the aspect of security a main concern of the network. Security and privacy are rapidly replacing performance as the first and foremost concern in many sensor networking scenarios. This work aims at enhancement of security done by increasing anonymity of sensor nodes. The nodes of a network may be prone to adversary attacks resulting in duplication of nodes. A scheme for improvement and detection of duplicate nodes are also done. The simulations are done in network simulator version2 (NS2) platform to evaluate the result of the system.**

Keywords—Anonymity, Wireless Sensor Network, Pseudonym, Duplicate Node, Clustering

I. INTRODUCTION

A wireless sensor network (WSN) consists of a number of sensor nodes that are deployed in an environment to perform the function of sensing data and reporting it. The sensing unit in the system senses the data from the surrounding environments of the WSN. Because sensor networks usually interact with sensitive data and operate in hostile unattended environments, it is imperative that the security concerns be addressed from the beginning of the system design. The extreme resource limitation of sensor devices poses considerable challenges to resource-hungry security mechanisms. The privacy preservation in the context of WSNs involves both privacy of monitored subjects and privacy of nodes and base stations.

A vast literature exists in this area of privacy preservation of WSN. Xiaoxin Wu [1] proposes an Anonymous Receiver-Contention Positioning (ARCPO) routing algorithm. The node identities (IDs) are kept anonymous. Pseudonyms, i.e., the positions of destinations, are used for data-packet delivery. The anonymity for a destination relies on the difficulty of matching its position to its ID by any observer. Another method is proposed by Ting Li et.al [2] where a cryptographic anonymity scheme in used. The author uses a lightweight dynamic pseudonyms based anonymous routing protocol, called DPAR where the security is implemented by lightweight symmetric key cryptography and hashing operations. The pseudonyms are generated by hashing operations and dynamically updated and synchronized by elaborate message interactions. Aparna Gurjar and A. R. Bhagat Patil [3] proposed a method for preserving source location privacy and implement it for WSNs given their operating constraints. This system uses a source location privacy scheme for WSN through cluster based anonymization. The scheme hides the real node identities during communication, by replacing them with random identities generated by the cluster heads. The degree of privacy of WSN is analyzed using entropy based method. Shi Leyi et.al [4] is using the technique of sensor anonymity enhancement scheme based on pseudonym (AESP) for clustered wireless sensor network with two phases, i.e., the communications within a cluster, and the communications over cluster heads or base stations. Pseudonyms are assigned and they are used to communicate between nodes in the network.

Due to the unattended nature of wireless sensor networks, an adversary can capture and compromise sensor nodes, generate replicas of those nodes, and mount a variety of attacks with the replicas that are injected into the network. These replica nodes can be identified using some particular mechanism. T. Nidharshini and V. Janani [5] uses sequential probability ratio testing (SPRT) and detects the duplicated nodes. After getting the secret key from the sensor node the sensitive data which is present in the nodes get leaked so an adversary can quickly degrades the network communication. To avoid this node compromised attack we use sequential probability ratio testing (SPRT). System detects replica node using the fact that a benign node should never move at speeds in excess of system configuration speed.

II. PROPOSED WORK

A wireless sensor network is clustered and the anonymity of the network is improved. The system uses pseudonym assignment to enhance the anonymity of the nodes of the network. Together with this, a duplicate node detection scheme is also proposed. The privacy of entire network is tried to improve.

A. Clustering of WSN

Clustering is done by dividing the entire nodes of the network into different groups by taking certain number of nodes together. This is done to increase the performance and

efficiency of the system. The grouping of nodes to different clusters can be done using different parameters. In this paper, we use low energy adaptive cluster hierarchy (LEACH) protocol as the basis. LEACH is a clustering-based protocol, which forms clusters on the basis of the received signal strength and uses the cluster head (CH) nodes as routers to communicate with base stations (BS). Each non-CH node finds out its cluster by selecting the CH that can be reached by using the lowest communication energy. After clustering the member nodes (MN) communicate with only the CH nodes. The cluster head nodes communicate and send data to base station. Figure1 shows a simple clustered WSN.

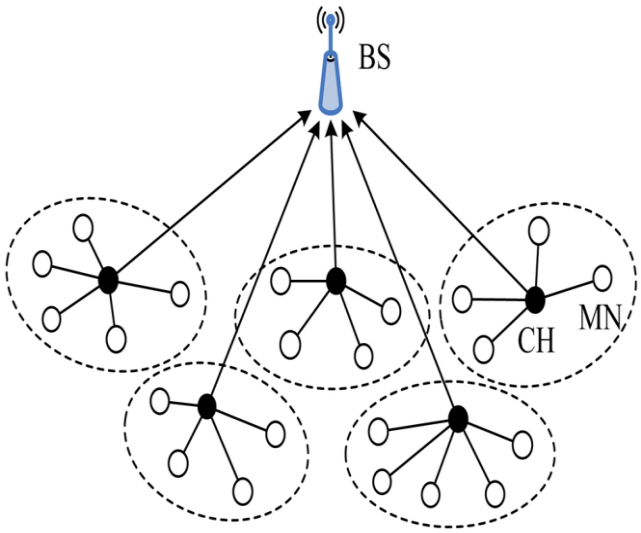

Figure 1: Clustering of WSN

B. *Anonymity Enhancement*

The anonymity enhancement is done using the pseudonym assignment. Each node in the network is assigned a unique pseudonym from the base station together with its identity during deployment. This pseudonym is used for the communications taking place in the network. The anonymity of the nodes in the system is improved as an entity outside the network cannot easily know about the pseudonym assigned to each node. Figure 2 shows process of pseudonym assignment.

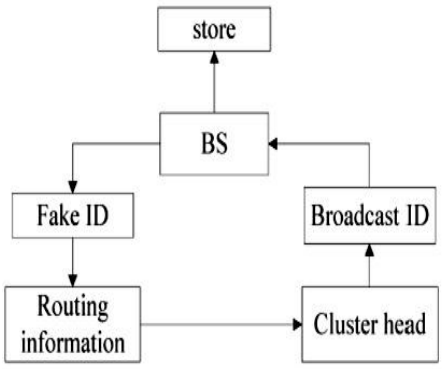

Figure 2: Process of pseudonym allocation [4]

C. *Detection of Duplicate nodes*

In wireless sensor networks, there are many nodes and they are unattended so an adversary can easily capture and compromise the sensor nodes and may make many replicas (duplicate) of them. After this, the sensor node's sensitive data which is present in the nodes get leaked so an adversary can quickly degrades the network communication. To avoid this node compromised attack we use basics of sequential probability ratio testing (SPRT) [5].

In this scheme, the base station calculates the speed of the network and set it as the configuration speed of the system.

$$\text{Speed}=\text{distance}/\text{time}$$

This configuration speed calculated for the whole network is set as threshold. The individual node speeds are measured separately and compared with this threshold. The base station computes the speed from every two consecutive claims of a mobile node and performs the SPRT by taking speed as an observed sample. Each time maximum speed is exceeded by the mobile node , base station accepts the hypothesis that the mobile node has been replicated. On the other hand, each time the maximum speed of the mobile node is not reached, it lead the base station to accept the hypothesis that mobile node has not been replicated (Figure 3).

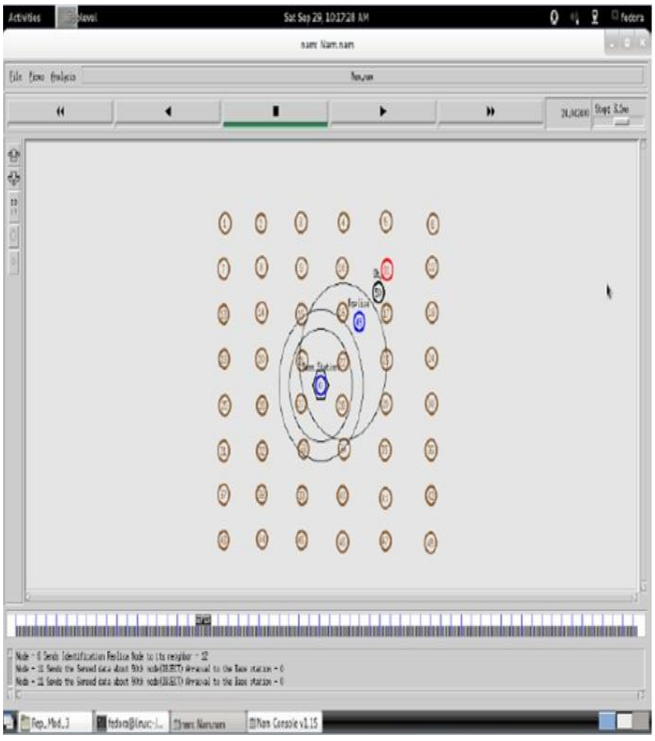

Figure 3: Detection of replica node [5]

III. SIMULATION AND RESULTS

The simulation of the work is done in NS2. The simulation is done for 55 nodes. The nodes are clustered to five different clusters (figure 4) and a base station is provided. Pseudonym assignment is shown using the text file where the assigned pseudonyms are saved (figure 5). The duplicate nodes are detected using the sequential probability ratio testing scheme (figure 6). The simulation of the system is shown in the network animator of the NS2 tool.

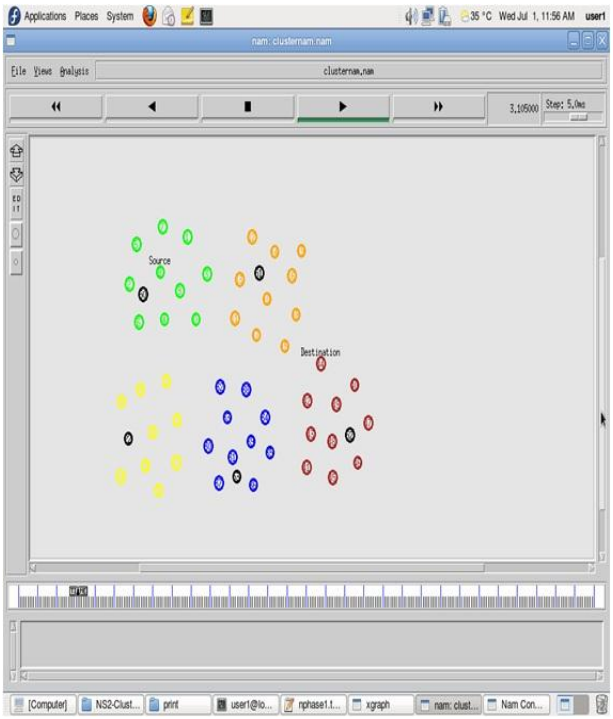

Figure 4: Screenshot of clustering in WSN

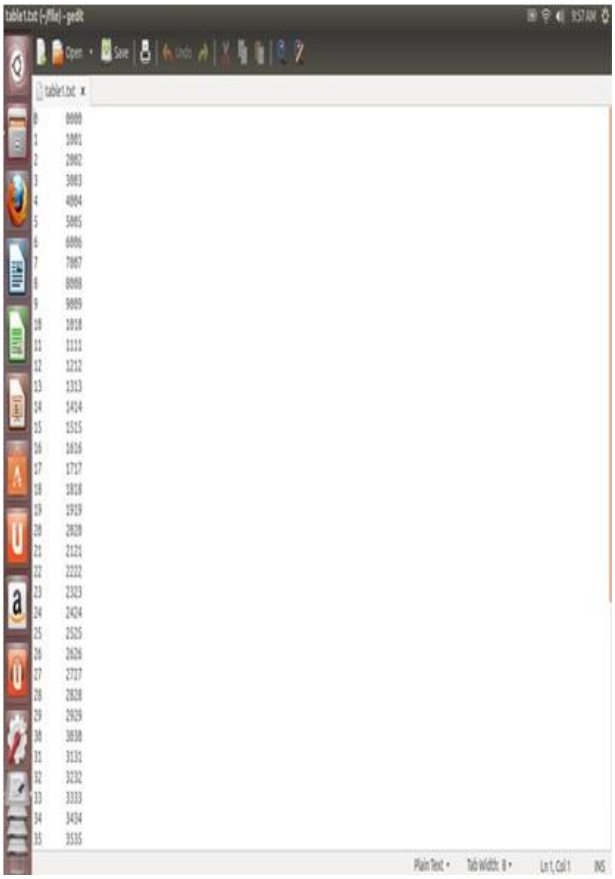

Figure 5: Screenshot of pseudonym assignment

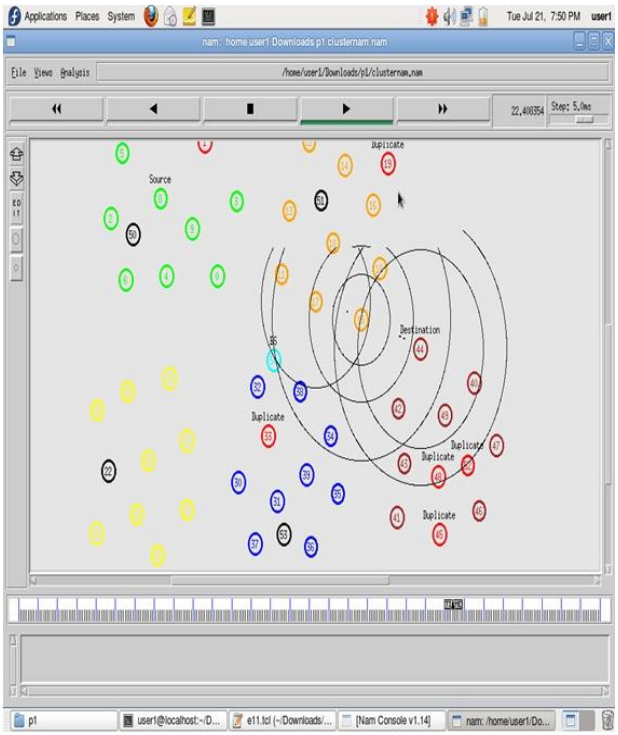

Figure 6: Screenshot of duplicate node detection

IV. CONCLUSION

Wireless sensor networks have seen extensive proliferation of applications and interest in research and industry. Unfortunately, WSNs have several limitations in terms of security that make them vulnerable to appropriating meaningful information especially in a malicious environment.

This paper aims in providing a privacy preserving method that is to be performed based on pseudonym assignment. The WSN is clustered based on the LEACH protocol. The system is further aiming to detect the compromised sensor nodes. Thus the anonymity of entire network is tried to be improved. The simulations are made in NS2 to show the designed system of wireless sensor network.

ACKNOWLEDGMENT

The authors are grateful to the Department of ECE of Sree Narayana Gurukulam College Of Engineering, Kadayirippu, Kerala for their kind support and permission to use the facilities available in the Institute.

REFERENCES

[1] Xiaoxin Wu. "Applying Pseudonimity for Anonymous Data Delivery in Location-Aware Mobile Ad Hoc Networks".., IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 55, NO. 3, MAY 2006.

[2] Ting Li, Yong Feng, Feng Wang, Xiaodong Fu., "A Dynamic Pseudonyms Based Anonymous Routing Protocol for Wireless Ad Hoc Networks ".,Yunnan Key Lab of Computer Technology Applications, School of Information Engineering and Automation, Kunming University of Science and Technology.

[3] GURJAR A, PATIL A. Cluster based Anonymization for Source Location Privacy in Wireless Sensor Network[J]. IEEE Communication Systems and Network Technologies (CSNT), 2013:248-251.

[4] SHI LeyP, FU Wenjingl, JIA Congl, LIU Xinl, JIA Chunfu, "A Sensor Anonymity Enhancement Scheme Based on Pseudonym for Clustered Wireless Sensor Network" College of Computer & Communication Engineering, China University of Petroleum**,**Qingdao, Shandong, P.R.China ,College of Computer & Control Engineering, Nankai University, Tianjin, P.R.China,.

[5] T. Nidharshini1, V. Janani ,"Detection of Duplicate Nodes in Wireless Sensor Networks Using Sequential Probability Ratio Testing"., International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 10, December 2012.

[6] Satyajayant Misra and Guoliang Xue*,"Efficient anonymity schemes for clustered wireless sensor networks"., Department of Computer Science and Engineering, Arizona State University, Tempe, Arizona, USA.

[7] J. Ho, M. Wright, and S.K. Das, "Fast Detection of Replica Node Attacks in Mobile Sensor Networks Using Sequential Analysis," Proc. IEEE INFOCOM, pp. 1773-1781, Apr. 2009.

[8] J. Ho, D. Liu, M. Wright, and S.K. Das, "Distributed Detection of Replicas with Deployment Knowledge in Wireless Sensor Networks," Ad Hoc Networks, vol. 7, no. 8, pp. 1476-1488, Nov. 2009.