International Journal of Electrical and Computer Engineering (IJECE)
Vol. 6, No. 4, August 2016, pp. 1570~1576
ISSN: 2088-8708, DOI: 10.11591/ijece.v6i4.10017

Implementation of Fuzzy Based Simulation for Clone Detection in Wireless Sensor Networks

Manjunatha R. C.[1], Rekha K. R.[2], Natraj K. R.[2]
[1] Department of Electronics and Communication Engineering, Research scholar, Jain University
[2] Department of Electronics and Communication Engineering, SJB Instutute of Technology
Bangalore, Karnataka, India

Article Info

Article history:

Received Jan 29, 2016
Revised Apr 2, 2016
Accepted Apr 14, 2016

Keyword:

Cluster
Fuzzy logic
Replica node detection
Trust aggregator
Wireless sensor networks

ABSTRACT

Wireless sensor networks are usually left unattended and serve hostile environment, therefore can easily be compromised. With compromised nodes an attacker can conduct several inside and outside attacks. Node replication attack is one of them which can cause severe damage to wireless sensor network if left undetected. This paper presents fuzzy based simulation framework for detection and revocation of compromised nodes in wireless sensor network. Our proposed scheme uses PDR statistics and neighbor reports to determine the probability of a cluster being compromised. Nodes in compromised cluster are then revoked and software attestation is performed.Simulation is carried out on MATLAB 2010a and performance of proposed scheme is compared with conventional algorithms on the basis of communication and storage overhead. Simulation results show that proposed scheme require less communication and storage overhead than conventional algorithms.

Corresponding Author:

Nataraj K R,
Proffesor and Head,
Department of ECE, SJB Institute of Technology,
Bangalore, Karnataka, India.
Email: Nataraj.sjbit@gmail.com

1. INTRODUCTION

Security is one of prime objective while designing any wireless sensor network architecture, especially when sensor network is exposed to hostile environment. In many of wireless sensor network applications such as military operations an adversary can capture any node and gain access to encryption keys. Once encryption keys are extracted adversary can create as many as replica nodes and deploy them at desired locations in the network. This type of attack is known as node replica attack and falls under the category of inside attacks. Node replica attack can cause severe damage to the system if left undetected. As these replica nodes gain the trust of neighbourhood nodes they can launch a verity of attacks including black hole attack, worm hole attack, false data injection, can divert network traffic towards the attacker, can leak secret information to the attacker etc.

The main problem in the detection of replication attack resides in the resource scarcity of sensor network. To effectively detect the repetitive use of same secret key network-wide comparison of location dependent authentication information is required. But limited memory and power supply put restrictions on the amount of authentication information stored and exchanged within the network. Hence energy efficiency, less storage and communication overhead will be the key issues in decidingutility of the algorithm. Node Replication attack has drawn interest of several researchers since last decade, protocols for detecting replication attack are categorized as centralized and distributed detection protocols. Centralized detection protocols such as Randomized key pre-distribution [1] and SET [2] use base station as centralise controlling

authority while distributed detection techniques such as Deterministic multicast [3], Randomized and Line selected multicast [4], RED [5] and localized multicast [6] uses witness based approach for clone node detection.

Existing detection techniques show a trade-off between detection accuracy and communication or storage overhead. Therefore this paper presents a fuzzy based architecture for detection of clone nodes in wireless sensor network. Our proposed scheme is extension of work presented by Geetha et al [7] and uses packet delivery ratio [PDR], trust values calculated by reporting and neighbouring cluster to detect replica nodes in a cluster based scenario. Rest of this paper is arranged as follows: Section –II discuss network and threat model, in section-III proposed fuzzy based replica node detection (FRND) protocol is given. Section-IV discuss simulation results and finally section-V concludes this paper.

2. NETWORK AND THREAT MODEL

2.1. Network Model

Consider a wireless sensor network with n nodes uniformly distributed in an area of 100x100 meter squares in a hostile environment. Network follows a cluster based architecture as shown in Figure 1, furthermore the network uses localization protocol and each node knows its location. Nodes are stationary after deployment and tied with RSA based public key cryptosystem.Base station is central and controlling authority which is responsible for all routing related task, furthermore at a fixed time interval each cluster send trust report to base station where FRND protocol is evaluated.

2.2. Threat Model

Let us assume that the attack has a partial control over the deployment region and may capture a subset of available nodes. After gaining access over secret keys, attacker may launch various inside attacks through compromised nodes. Furthermore it is also assumed that each compromised node is surrounded by at least one legitimate node [4].

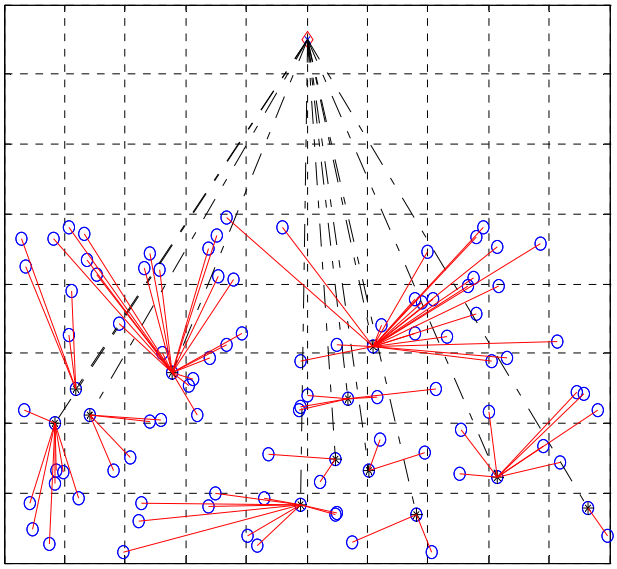

Figure 1. Network arrangement

3. FUZZY BASED REPLICA NODE DETECTION SCHEME (FRNDS)

Fuzzy based replica node detection (FRND) protocol adopts a region based approach for detection of compromised nodes operating in the environment. The algorithm divides the network area into a number of regions; with each region has a clusterhead node with some common nodes sharing between the other regions.The algorithm relies on trust value for each cluster and detects the cluster trustworthiness based on the cluster trust value. Once a cluster is flagged to be untrustworthy, software modules of all the sensor nodes belonging to that cluster is tested by the network operator followed by the detection and revocation of compromised nodes in that cluster. A simple approach for untrustworthy cluster detection might be based on

comparing a single trust value with a threshold; however with this approach an error in cluster trust calculation will directly affect the output of the algorithm. To minimize the impact of such errors FRND protocol uses multiple trust values and packet delivery ratio to decide whether the cluster is trustworthy or not. Multiple trust values are collected from trust aggregator present in same cluster as well as the overlapping nodes of the neighbouring cluster. Fuzzy based approach is applied to compromise node detection and revocation as follows: each node in a cluster is act as a trust aggregator in round robin manner. In each time span, the trust aggregator computes trust value and packet delivery ratio for its cluster and report it to the base station. The base station than perform FRND protocol to evaluate cluster's trustworthiness; once a cluster is decided to be untrustworthy, the network operator performs software attestations against all sensor nodes to detect and revoke the compromised nodes in that cluster.

The detailed description of fuzzy based replica node detection protocol is given as follows: Prior to the deployment, each node in the networks is allotted a unique ID and network is divided into number of overlapping clusters. Communication cost of the system will dependent on cluster size, although there is no restriction over the size and the shape of the cluster but an increase in cluster size will increase intra communication cluster cost as the local trust report will require more hopes to reach at the trust aggregator. While keeping cluster size small it will be difficult to detect compromise nodes. Furthermore, secret keying material is preloaded into each sensor node for pair wise key establishment by base station [8],[9]. The entire process can be described in three steps.

3.1. Cluster formation and Trust aggregator selection

After deployment, each node determines its location and finds out the cluster to which it belongs, this cluster is referred to as home cluster to the node while other clusters will be foreign clusters. The sensor node then discovers the ID of all the neighbouring nodes in its home cluster and establishes pair wise secret keys with them. Selection of trust aggregator is done then in a round robin manner as follows: each cluster is associated with a series of time slots; in a pseudo random order each node decides its duty timeslot and act as a trust aggregator. These trust aggregator nodes are responsible for the sending trust reports and PDR characteristics to the base station.

3.2. Trust calculation and Forwarding

In each time interval T_i, neighbourhood trust is computed by each cluster C in every node. Neighbourhood trust is defined as the difference between the probability distributions of the information generated and information sent to the node in consideration by its neighbouring node in current cluster. Neighbouring trust is related to the authenticity of node and it increases with data transmission between neighbouring nodes. The trust information can also be transmittedto the base station by the nodes of neighbouring cluster which are one hop away from the current cluster. The arrangement is given in Figure 2.

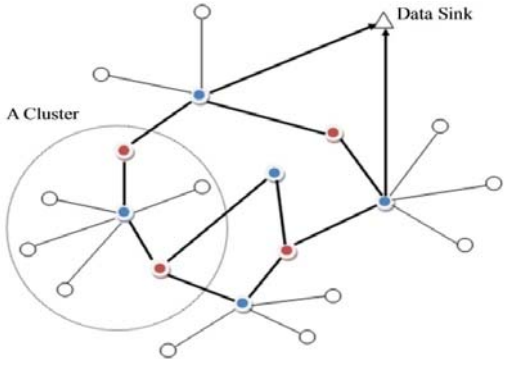

Figure 2. Clustered network with nodes overlapping Clusters [10]

3.3. Compromise Node Detection and Revocation

Once a cluster-trust statement is received at the base station by the trust aggregator node of current cluster; firstly its authenticity and the freshness of the report is checked at the base station. For authenticity secret key shared between the base station and trust aggregator is checked whereas for freshness of the report timer associated with it is checked. Unauthentic or expired reports are discarded by the base station. For the detection of compromised trust aggregator, the base station maintains the record of each trust aggregator by

binding its ID to its home cluster. This will prevent a compromised trust aggregator from claiming multiple home clustersand launching replay attack with fake cluster-trust statements.

To handle the non-linearity associated with the problem a fuzzy based approach is presented in this research. FIS architecture is proposed for the detection of untrustworthy cluster on the basis of trust reports from same and neighbouring cluster and packet delivery ratio (PDR) statistics of the cluster under consideration. Cluster formation is more efficient using fuzzy logic [11].

The architecture of proposed system is given in Figure 3, with trust report from cluster under consideration and its immediate neighbour and packet delivery ratio being the input to the system. The output of the system is the probability that the cluster is trustworthy or not. The proposed FIS structure is based on the set of rules given in Table 1. Based on the rule set the probability of a cluster being untrustworthy is calculated, if detected untrustworthy software attestation is performed over the node of cluster in consideration.

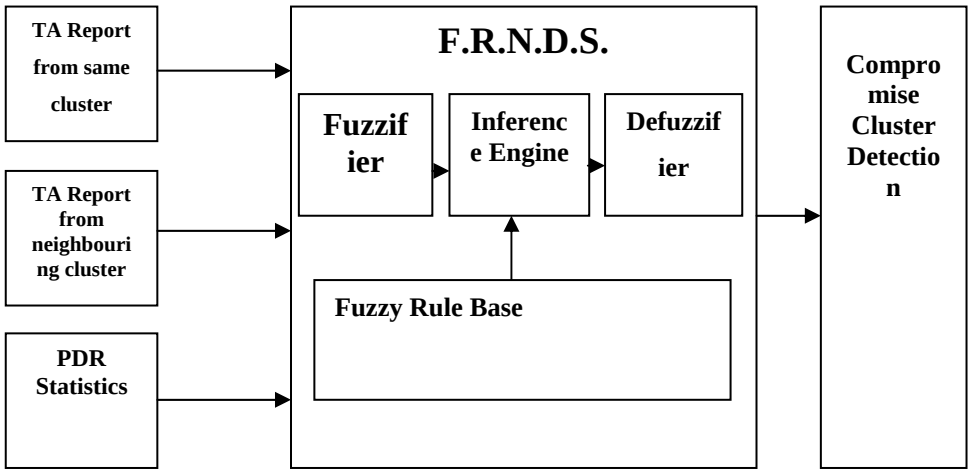

Figure 3. Fuzzy logic based Replica Node Detection Scheme (F.R.N.D.S.)

Table 1. Rule set for proposed system

S. No.	TA Report from same cluster	TA Report from neighbouring cluster	PDR Statistics	Cluster Trustworthiness
1	Low	Low	Low	Low
2	Low	Low	Medium	Low
3	Low	Low	High	Low
4	Low	Medium	Low	Low
5	Low	Medium	Medium	Medium
6	Low	Medium	High	Medium
7	Low	High	Low	Medium
8	Low	High	Medium	Medium
9	Low	High	High	Medium
10	Medium	Low	Low	Low
11	Medium	Low	Medium	Low
12	Medium	Low	High	Medium
13	Medium	Medium	Low	Low
14	Medium	Medium	Medium	Medium
15	Medium	Medium	High	Medium
16	Medium	High	Low	Medium
17	Medium	High	Medium	Medium
18	Medium	High	High	High
19	High	Low	Low	Low
20	High	Low	Medium	Low
21	High	Low	High	Medium
22	High	Medium	Low	Low
23	High	Medium	Medium	Medium
24	High	Medium	High	Medium
25	High	High	Low	Medium
26	High	High	Medium	High
27	High	High	High	High

4. SIMULATION RESULTS

To evaluate the performance of proposed fuzzy based replica node detection protocol, MATLAB based framework has been presented. The performance criterion is set to communication overhead and storage overhead. Communication overhead being the number of messages transmitted and storage overhead being the memory required by each node, Let n being the number of nodes presented in the network, d being average degree of neighbourhood, p being the probability of clusterhead election and g and Sbeing the number of witness nodes and number of clusterhead reporting to base station the communication and storage overhead can be computed as follows:

Table 2. Simulation Parameter

n	100:100:1000
d	40
p	0.05
g	2
S	1
C	$p * n$

Based on the computational formula given in Table 3, communication and storage overhead of different algorithms have been calculated and compared with proposed fuzzy based replica node detection scheme. Figure 4 indicates the proposed model of fuzzy based replica node detection system consisting three input parameters like Trust agreegat from same cluster, Trust agreegate from neighbouring cluster and Packet delivery ratio.

Table 3. Comparison of communication and communication overhead

Parameter / Method	Broadcast	Centralise Detection	Deterministic Multicast	Randomised Multicast	Line selected Multicast	Proposed scheme
Communication Overhead	n^2	$n\sqrt{n}$	$\sqrt{n}$	n^2	$n\sqrt{n}$	$C\sqrt{n}$
Storage Overhead	d	d	g	$\sqrt{n}$	$\sqrt{n}$	S

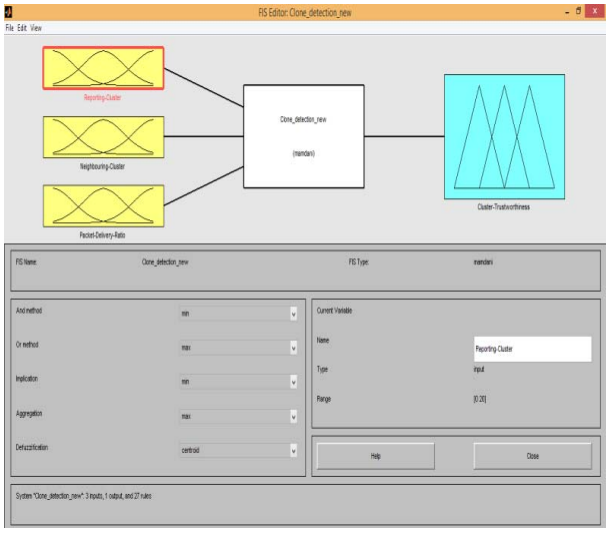

Figure 4. Proposed fuzzy based replica node detection system

Simulation results given in Figure5 and 6 show that proposed scheme requires less communication and storage overhead. Let n=100, d=40, p= 0.05, g=2 and s=1, the communication overhead for broadcast method will be 10, centralise detection will be 100, deterministic multicast will be 10, randomised multicast will be 1000, line selected multicast will be 100 and for proposed scheme will be 5. Furthermore storage

overhead for broadcast method will be 40, centralise detection will be 40, deterministic multicast will be 2, randomised multicast will be 10, line selected multicast will be 10 and for proposed scheme will be 1.Comparative graph for communication and storage overhead are given in Figure 5 and 6 respectively.

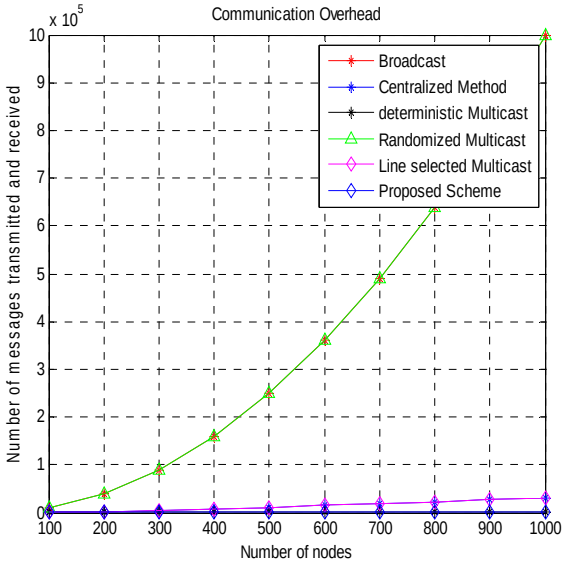

Figure 5. Comparison of communication overhead

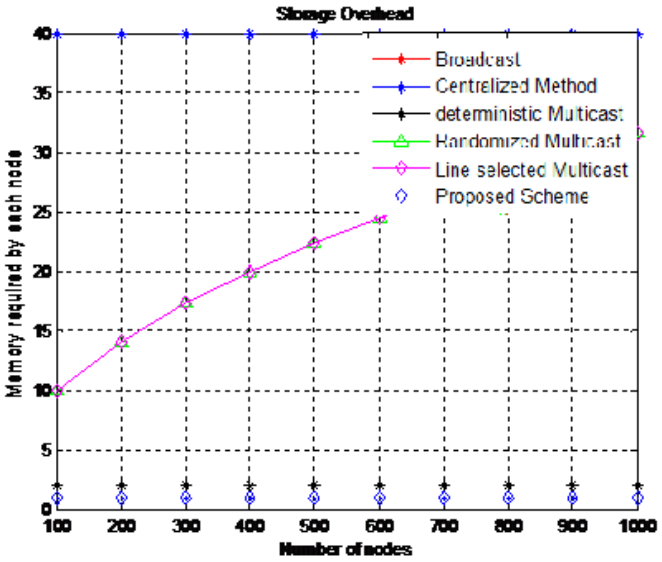

Figure 6. Comparison of Storage overhead

5. CONCLUSIONS

This paper presents simulation framework for fuzzy based replica node detection scheme in clustered wireless sensor networks. The proposed scheme uses packet delivery ratio (PDR) and trust reports to determine the probability of a cluster being compromised. Performance of proposed scheme is compared with broadcast, centralize detection, randomized multicast, deterministic multicast and line selected multicast methods on the basis of communication and storage overhead required by the algorithm. In conventional algorithms communication and storage overhead is function of number of nodes presented in the system, average degree of neighborhood and number of witness nodes whereas in proposed scheme both are function of number of clusters present and number of reporting clusters in neighborhood. Simulation results shows

that with same parameters taken; proposed scheme requires less communication and storage overhead than conventional algorithms.

REFERENCES

[1] R. Brooks, *et al.*, "On the detection of clones in sensor networks using random key predistribution," *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, vol/issue: 37(6), pp. 1246-1258, 2007.

[2] H. Choi, *et al.*, "SET: Detecting node clones in sensor networks," *Security and Privacy in Communications Networks and the Workshops, 2007, Secure Comm 2007, Third International Conference on*. IEEE, 2007.

[3] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," *Proceedings of the 9th ACM conference on Computer and communications security*, ACM, 2002.

[4] B. Parno, *et al.*, "Distributed detection of node replication attacks in sensor networks," *Security and Privacy, 2005 IEEE Symposium on*. IEEE, 2005.

[5] M. Conti, *et al.*, "A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks," *Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing*, ACM, 2007.

[6] B. Zhu, *et al.*, "Localized multicast: efficient and distributed replica detection in large-scale sensor networks," *Mobile Computing, IEEE Transactions on*, vol/issue: 9(7), pp. 913-926, 2010.

[7] R. Geetha, *et al.*, "Fuzzy logic based compromised node detection and revocation in clustered wireless sensor networks," *Information Communication and Embedded Systems (ICICES), 2014 International Conference on*. IEEE, 2014.

[8] T. Park and K. G. Shin, "Soft tamper-proofing via program integrity verification in wireless sensor networks," *Mobile Computing, IEEE Transactions on*, vol/issue: 4(3), pp. 297-309, 2005.

[9] A. Seshadri, *et al.*, "Swatt: Software-based attestation for embedded devices," *Security and Privacy, 2004, Proceedings, 2004 IEEE Symposium on*. IEEE, 2004.

[10] M. Beldjehem, "Toward a Multi-Hop, Multi-Path Fault-Tolerant and Load Balancing Hierarchical Routing Protocol for Wireless Sensor Network," *Wireless Sensor Network*, 2013.

[11] A. K. Kaushik, "A Hybrid Approach of Fuzzy C-means Clustering and Neural network to make Energy-Efficient heterogeneous Wireless Sensor network," *International Journal of Electrical and Computer Engineering (IJECE)*, vol/issue: 6(2), 2016.

BIOGRAPHIES OF AUTHORS

Manjunatha R C obtained his B.E and M.Tech Degree from Visveshwaraya University, Karnataka, India, in 2006 and 2008 respectively in Telecommunication Engineering. He is working as Assistant professor at Acharya Institute of Technology, Bangalore, and Karnataka. He is currently pursuing his Ph.D at Jain University, Karnataka. His current research includes Clone detection in wireless Sensor Networks. He is a member of ISTE and IE.

Dr K. R. Rekha obtained her ME degree from Bangalore University, India in 2000. She is working as a Professor in the Department of Electronics and Communication in SJB Institute of Technology, Bangalore. She has pursued her Ph. D. degree in Dr MGR University, Chennai. Her research interests include Wireless communication, FPGA implementation, and Microcontroller and Embedded system design. She is a member of MIE, MISTE and IETE

Dr K. R. Nataraj obtained his ME degree from Bangalore University, India in 2000. He worked as Professor and Postgraduate Coordinator in the Department of Electronics and CommunicationEngineering. Currently he is Head of the Department in SJB Institute of Technology, Bangalore. His research interests include Wireless communication, FPGA implementation, and Microcontroller and Embedded systems design. He is a member of MIE, MISTE , IETE and IEEE