Trust Factor based LEACH-C protocol for Wireless Sensor Networks

Geetha V
National Institute of Technology, Karnataka
Surathkal, Mangalore.
D.K. Karnataka - 575 025

K. Chandrasekaran
National Institute of Technology, Karnataka
Surathkal, Mangalore.
D.K. Karnataka - 575 025

ABSTRACT

Trust in wireless sensor network is an essential feature to detect various kind of attacks in the network. Wireless sensor nodes are more prone to attacks as nodes are deployed in an open environment. In case of centralized low energy adaptive cluster head protocol cluster heads in each round are selected by sink node. We propose a trust factor based LEACH-C protocol, to detect malicious nodes based on trust calculations which involves observation of various parameters and evaluation of trust factors. Simulation is conducted in using NS-2, by varying the number of malicious nodes and results are analyzed for energy consumption, number of data packets sent and percentage of malicious node detection.

General Terms:

Trust Management, LEACH-C

Keywords:

Centralized - Low Energy Adaptive Cluster Head protocol (LEACH-C), Trust management, Trust Factors, Wireless sensor networks

1. INTRODUCTION

Hierarchical cluster based routing protocols are more suitable for wireless sensor network as nodes are randomly deployed in an open environment. If locality of reference is applicable to the application of wireless sensor network, then the sensor nodes can form clusters, collect data from neighbor nodes and aggregate data before sending it to sink node. Data aggregation also reduces the number of communications in the network, as the cluster heads are responsible for sending data to sink node. As a result of reduction in the total number of communications, the total lifetime of a network increases as it reduces the energy required to transfer information to sink node. As the nodes are deployed in open environment the nodes are more prone to different kind of attacks. Identification of such kind of attack and eliminating those nodes from further interaction in the network provides better results in the network.

LEACH-C is similar to LEACH [1] protocol, where instead of distributed method to find cluster heads like LEACH, LEACH-C uses centralized approach to find cluster heads for each round. In LEACH-C protocol, all sensor nodes communicate their position information and energy level to the base station and provide the necessary information to calculate the average node energy. Sensor nodes with remaining energy less than the calculated average node energy are restricted from becoming the cluster head during the current round. Base station finds the predefined number of cluster heads and divides the network into clusters, so as to minimize the energy required for non-cluster head member to transmit their data to the respective cluster heads. LEACH-C assumes that every node knows its location in priori. Hence, cost is imposed due to nodes as they use a GPS receiver to find their location information. The functioning of the protocol in each round consists of the following four phases:

(i) Advertisement phase: Every node of the network sends its information regarding the current energy level and location to base station. The base station analyzes the details and selects the most suitable cluster heads for that round. After selecting cluster heads, the base station broadcasts this information to every node in the network in the form of a list containing node-id of cluster head.

(ii) Cluster setup phase: Each node receives the cluster head list broadcasts by the base station. If the nodes own id is present in the list, then that node becomes cluster head for that particular round.

(iii) Schedule Creation: Every non cluster node identifies its TDMA schedule and its cluster head from the information broadcast by the base station.

(iv) Data Transmission: The Cluster head receives data from the node at its assigned time slot, aggregates and/or sends it to the base station. After a certain predefined time, the next round begins with the advertisement phase.

The network is prone to various kinds of attacks as the nodes may be deployed open environment. A compromised sensor node may host various kinds of attack in the network. In this aspect, any sensor network must be able to detect various kinds of attacker nodes. The cryptography technique may not provide a complete solution for all kinds of attacks. The trust based protocols proved better results in social networks, p2p networks, wireless networks, MANETs and wireless sensor networks. It is not sufficient to build the trust management system based on one or two parameters. The network must be able to find trustworthiness

of the node based on various parameters and trust factors. We propose a trust factor based LEACH-C by considering various parameters and trust factors. We would like to mention that, as of our knowledge, trust based LEACH-C is a newly proposed work.

Section 2 provides related work about LEACH and LEACH-C with respect to trust management. Section 3 explains our proposed trust factor based LEACH-C protocol. Section 4 discusses about simulation experiments and results followed by conclusions and references.

2. RELATED WORK

The survey on the various trust management system for wireless sensor network is provided in [2]. The possible type of inside and outside attacks in any wireless sensor network and method required to solve the issues mentioned briefly. In [3] a trust based LEACH protocol is proposed. The direct and indirect trust is used to evaluate the trustworthiness of the nodes. Each TDMA round contains a data slot and trust slot where the trust slot is used to exchange trust information among nodes. The cluster head selection is based on decision trust. However, the communication among nodes for exchange of trust information is more as it also takes indirect trust into account. Watchdog LEACH is proposed in [4] in which few nodes are elected as watchdog nodes to monitor the network. Further analysis of various attack detection is required over watchdog nodes. In [5] the trust is calculated in hierarchical levels between sensor node to cluster head and cluster head to sink node. The technique is applied for geographical routing and intrusion detection. In [6] LEACH and LEACH-C protocols are compared. The results show that the energy dissipation in each round for LEACH-C is more and uniform compared to LEACH. But the lifetime of LEACH-C is better compared to LEACH. The work in [7], [8] and [9] proposes snooze attack, HELLO flood attack and denial of sleep attack respectively. Monitoring nodes on various parameters improves identification of various kinds of attacks.

3. OUR WORK: TRUST BASED LEACH-C PROTOCOL

Trust in wireless sensor network plays an important role in identifying various types of malicious behavior of nodes. In this section, following things are discussed in detail: type of attacks possible in LEACH-C, trust in wireless sensor networks, and various factors which influences on the trust value of a node in wireless sensor network.

3.1 Attacker model for LEACH-C

(1) Attack related to communication: Sink node identifies cluster heads based on its energy. After a cluster head node joins to sink node, it has to send aggregated data to sink node. A cluster head may drop packets without sending it sink node. Similarly, a sensor node may join to cluster head, and may not send data to its respective cluster heads. In both cases, the data gets lost and the CH or Sink node may not be able to predict the behavior of the node. By saving energy a node gets more chance to become cluster head, in the next rounds.

(2) Attack related to data aggregation: A sensor node can send fake data to cluster head, so that the aggregated value of data gets altered, which further leads to wrong information at sink node.

3.2 Parameters and Trust factors for LEACH-C

To identify various attacks the sensor node has to observe its neighbor based on parameters. In any routing protocol for wireless sensor network, one can observe on parameters such as : number of forwarded packets (P_{fwd}), Number of broadcast messages (P_{br}), Number of routing packets transferred (P_{rt}), Number of times the data is consistent (P_{data}), Number of times location of the node is consistent (P_{loc}), number of times the node was available (P_{av}). Among all these parameters only very few parameters are suitable for LEACH protocol. In LEACH-C protocol the communication happens only with two hops: sensor node to cluster head, cluster head to sink node or base station. Hence, the cluster node and sink node has to monitor the nodes regarding communication aspects (P_{fwd}). The cluster head should be able to identify the data stealthy attack. To identify such attacks, a cluster head has to monitor the data (P_{data}). As LEACH-C is not multihop protocol, finding route is not an issue, hence (P_{rt}) does not have much significance in LEACH-C protocol. The LEACH protocol considers the location of the node based on received information from each sensor node. Hence, the observation on a parameter (P_{loc}) is also important. The availability of a node depends on the energy of the node. So the energy (P_{av}) of neighbor is monitored to check availability of nodes.

To evaluate trustworthiness of a node in wireless sensor network, following trust factors are necessary: Communication, Data, Functionality, Location, Energy, Trust update, and Risk. Evaluation of all these seven trust factors and combining them together helps to evaluate the trustworthiness of sensor nodes in the network. Each of these trust factors is identified as $T_{communication}$, T_{data}, $T_{functionality}$, T_{loc}, T_{energy}, T_{risk}. Even though trust update is a factor which influences on the total trustworthiness of a node in the network, it is used as a variable for factor to analyze the performance of the network.

Trust can be calculated based on the beta reputation system in [10],[11]. The indirect trust takes an important role when the nodes are highly mobile, as it allows the node to converge to decide about trustworthiness of a node as early as possible. Hence mos tof the sensor networks are static wireless sensor network, it is sufficient to consider only direct trust for trust evaluation. Each operation is considered as "successful" (α) or "unsuccessful" (β) operation. Trust is calculated as shown in equation 1, where Trust(i,p) indicates the trust value of the node *i* for parameter *p*.

$$Trust(i,p) = (\alpha + 1.0)/(\alpha + \beta + 2.0) \quad (1)$$

3.3 Trust Factor Based LEACH-C Protocol (TF-LEACHC)

We propose a trust factor based secure communication based LEACH-C for wireless sensor network. Every node sends the necessary information to sink node in each round. The sink node monitors the sensor nodes in the network at each TDMA schedule. Any node identified as malicious will be eliminated from further involvement in the network. The phases of TF-LEACHC are as follows.

(i) Advertisement phase: Every node of the network sends its information regarding the current energy level and location to the base station. The base station analyses the details and provide the most suitable cluster heads for that round. Selection of cluster head is based on energy as well as trust of that particular

node. After selecting cluster heads, the base station broadcasts this information to every node in the network in the form of a list containing node-id. If any node is identified as malicious node based on low trust value, then that node is excluded from the list. As a result, malicious nodes are not selected for further rounds in wireless sensor network.

(ii) Cluster setup phase: Each node receives the cluster head list broadcasted by the base station. If the nodes own id is present in the list, then that node becomes cluster head for that particular round.

(iii) Schedule Creation: Every non cluster node identifies its TDMA schedule and its cluster head from the information broadcast by the base station.

(iv) Data Transmission: The Cluster head receives data from the node at its assigned time slot. The cluster head maintains the record of the number of times data received by a sensor node, and the number of times data not received by sensor node in a given TDMA slot. The cluster head can aggregate the data and send it to the base station. At the end of each TDMA round, the cluster head sends the node id of nodes which have not sent the data to cluster head. After a certain predefined time, the next round begins with the advertisement phase. The trust value is calculated at the completion of each TDMA schedule.

(v) Trust calculation: The cluster head maintains information of every node in a table. The fields of the table contains nodeid α and β values, *r*, *s* for each trust factor. The NodeID represents the ID of the node, α represents the number of times the operation was successful, β represents the number of times the operation was not successful upto last TDMA schedule, *r* represents the number of times operation was successful in this current TDMA schedule, and *s* represents number of times the operation was not successful in this current round. Initial values for α and β are taken as 1. If the node id is specified in the malicious list sent by cluster head, then *s* value of the corresponding trust factor of the node in the table is incremented by 1, else *r* value is incremented. The α and β values of a trust factor are updated as shown in equation 2 and 3, where W is the weight or aging factor [6,7] and $\alpha(i,p)$, $\beta(i,p)$ indicates successful and unsuccessful operations observed for node *i* for parameter *p* up to last TDMA schedule, and $r(i,p)$, $s(i,p)$ indicates successful and unsuccessful operation in one TDMA schedule.

$$\alpha(i,p) = W * \alpha(i,p) + r(i,p) \tag{2}$$

$$\beta(i,p) = W * \beta(i,p) + s(i,p) \tag{3}$$

The trust value of a node is calculated at the end of each TDMA schedule. If the trust value of a particular node goes below a certain threshold, then the corresponding flag value will be set to 1, indicating the node is detected as malicious. The Node energy is the energy of that particular node at the end of last round. If a node is detected as malicious, the cluster head sends nodeID of malicious nodes along with aggregated data to base station. The base station eliminates these nodes for further processing in successive rounds.

4. SIMULATION RESULTS AND DISCUSSIONS

Network Simulator (NS) version 2.34 [12] is used for simulating the protocol with mit patch. Simulations are carried out by keeping the number of nodes and simulation time as a constant. The simulation parameters are shown in table 4.

Table 1. Simulation Parameters

Simulation Parameters	Value
Simulation Time	1000 sec
Topology size	1000 X 1000 m^2
Number of Nodes	100
Number of Clusters	4-8
Initial node energy	2 joule
Nodes Distribution	Uniformly Distributed
BS Position	Located at (50,50)

The simulation experiments are conducted by considering 10%, 20% and 30% communication malicious nodes and data stealthy attacks. The malicious nodes does not forward the data packets to sink node. The data stealthy attacker node sends unrelated data to the cluster head to affect the data aggregation value. The results are analyzed for total energy consumption, total number packets sent in the network, total number of data packets dropped in the network. The results are also analyzed for percentage of true positive malicious node detection in the network. To compare our proposed protocol, with original LEACH-C and LEACH-C without trust calculation, a mixed mode of 10% communication malicious and 10% of data stealthy attacker nodes are considered in the simulation.

Figure 1 to 6 shows the results of 10%, 20% and 30% communication malicious and data stealthy attacker nodes. Figure 1 shows total energy consumption and figure 2 shows the total number of data packets sent in the network, with 10%, 20% and 30% communication malicious nodes in the network for LEACHC and TF-LEACHC protocol. As the number of communication malicious nodes increases, the energy consumption decreases in case of LEACHC.

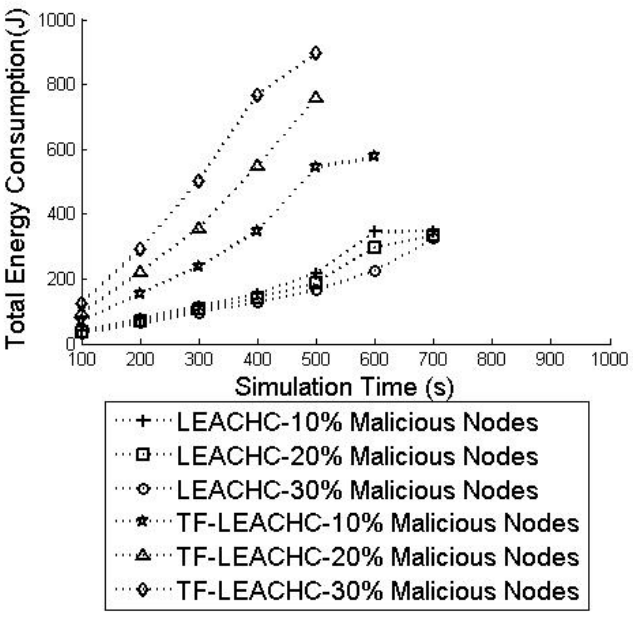

Fig. 1. Total energy consumption for 10%, 20% and 30% communication malicious nodes in the network

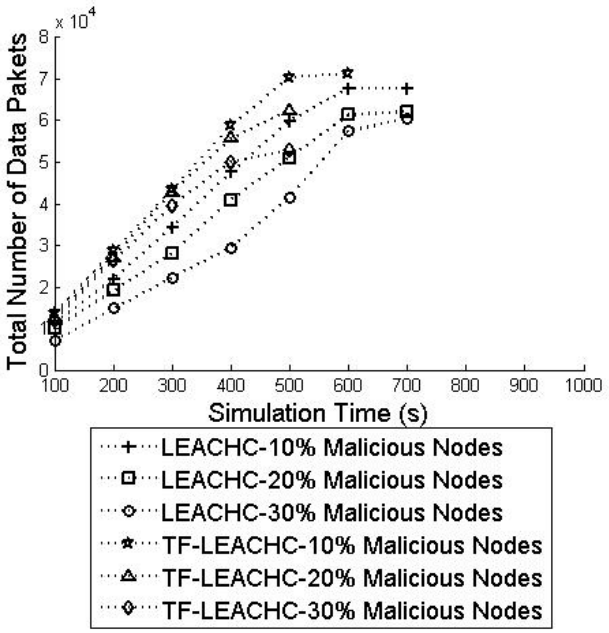

Fig. 2. Total data packets sent in case of 10%, 20% and 30% communication malicious nodes in the network

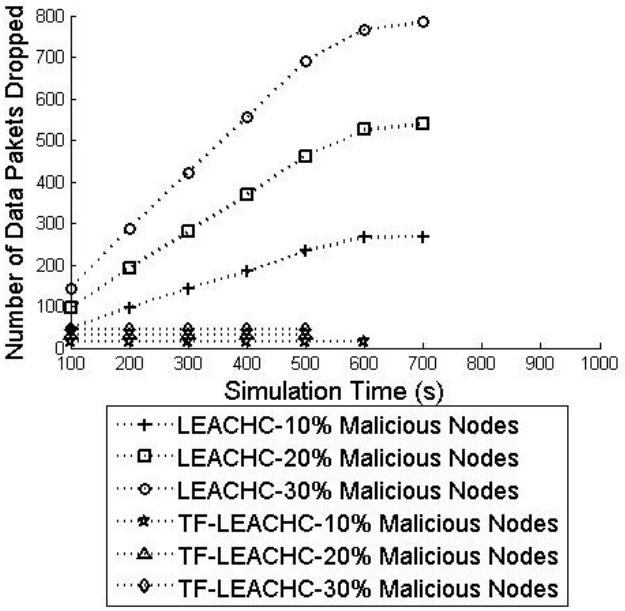

Fig. 3. Total number of packets dropped in the network in case of 10%, 20% and 30% communication malicious nodes in the network

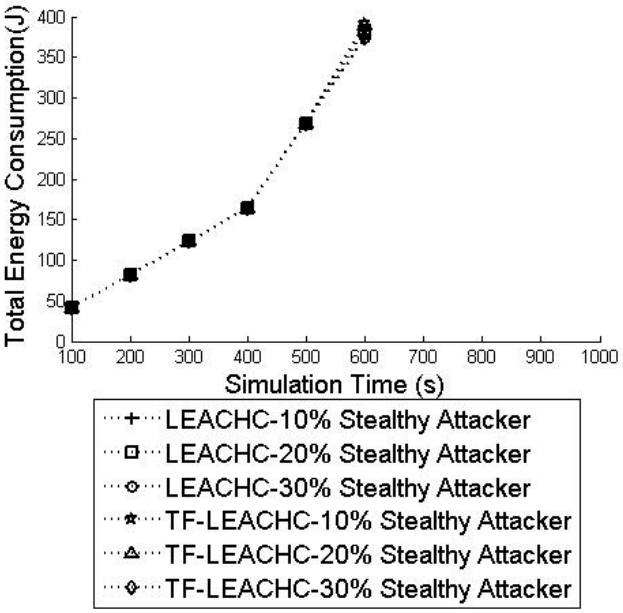

Fig. 4. Total energy consumption for 10%, 20% and 30% data stealthy attacker nodes in the network

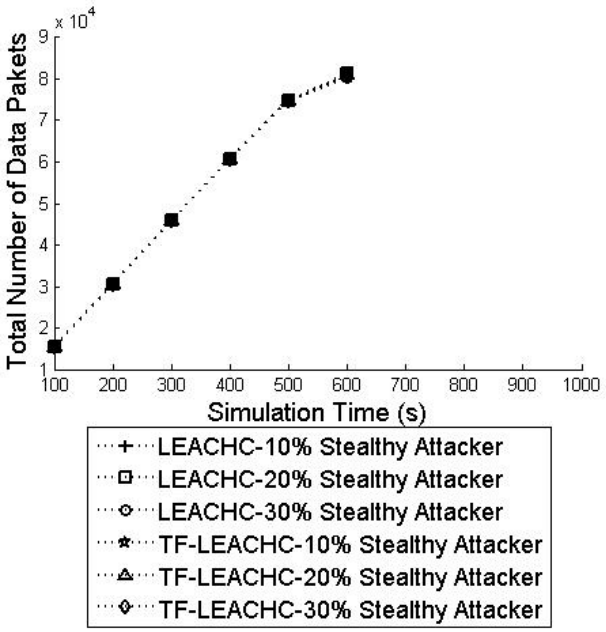

Fig. 5. Total data packets sent in case of 10%, 20% and 30% data stealthy attacker nodes in the network

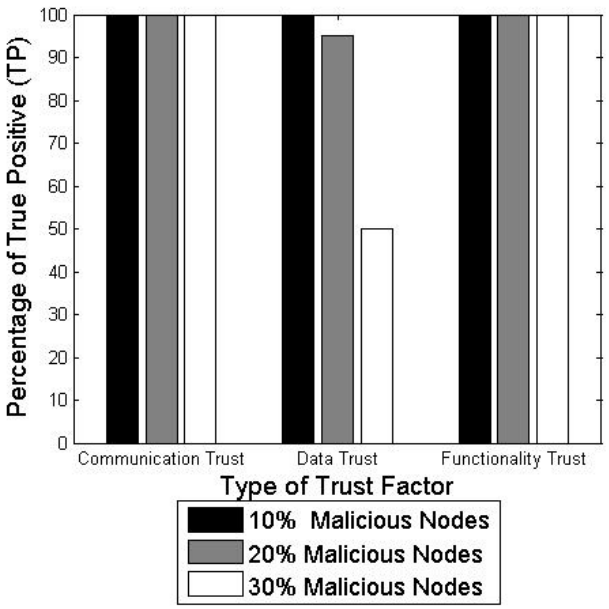

Fig. 6. Percentage of true positive detection in case of 10%, 20% and 30% data stealthy attacker nodes in the network

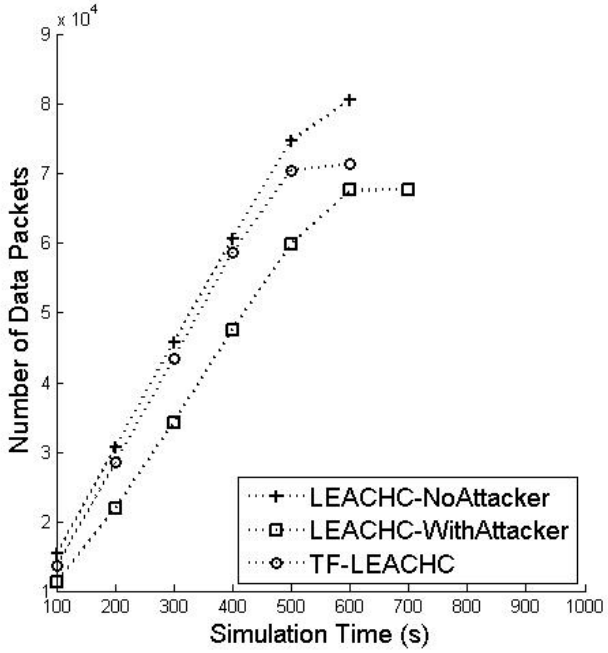

Fig. 8. Total number of data packets sent in case of 10% communication and 10% data stealthy attacker nodes in the network

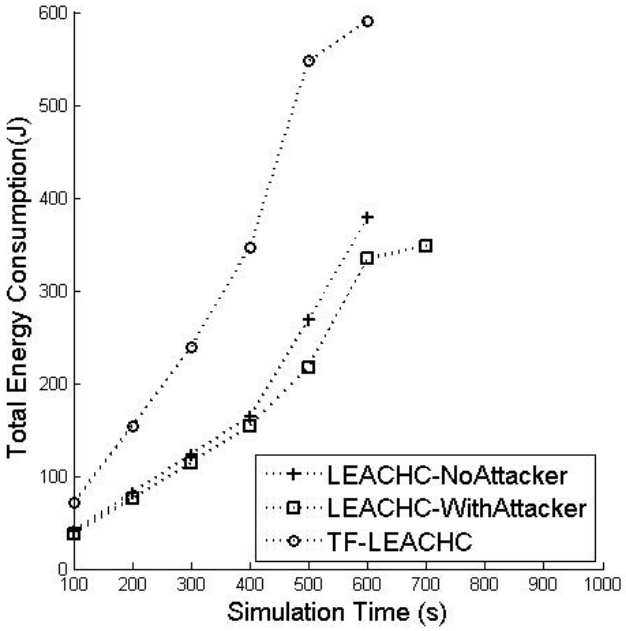

Fig. 7. Total Energy consumption in case of 10% communication and 10% data stealthy attacker nodes in the network

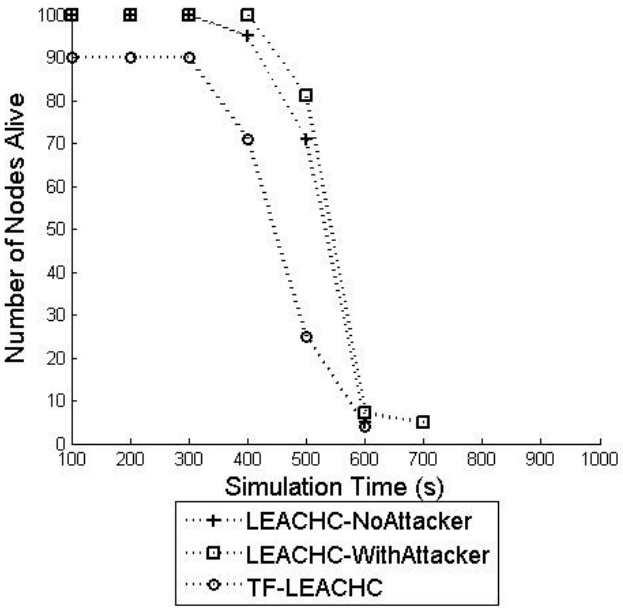

Fig. 9. Total number of nodes alive in case of 10% communication and 10% data stealthy attacker nodes in the network

The energy consumption increases in case of TF-LEACHC due to communication of malicious node information to SINK node in each TDMA schedule. However, the total number of data packets increases in case of TF-LEACHC compared to LEACHC as shown in figure 2. As the malicious nodes get detected and the nodes are eliminated, the remaining nodes helps to the healthy functioning of the network. Figure 3 shows that the number of packets dropped in case of TF-LEACHC is constant compared to LEACH, as the malicious nodes are eliminated from the network, as soon as they get detected.

Figure 4 and 5 show results of total energy consumption and total number of data packets sent in the network in case of 10%, 20% and 30% data stealthy attacker nodes. The data stealthy attacker node sends data to CH node, with some fake data. As a result, there is no much change in energy consumption as well as the number of data packets sent in the network even with the increase of the number of data stealthy attacker nodes. The main issue is the aggregation value at CH gets effected due to fake data. Figure 6 shows the percentage of true positive detection in case of 10%, 20% and 30% data stealthy attacker nodes in the network. The communication trust detects communication malicious node with 100%, functionality trust detects functional maliciousness 100%, however the percentage of data stealthy attacker detection decreases as the number of attacker node increases. With 10% malicious node the detection is 100% with a malicious detection threshold of trust value =0.35.

Figure 7, 8 and 9 shows the results of energy consumption, total number of data packets sent, and number of nodes alive in the network, in case of 10% communication and 10% data stealthy attacker nodes in the network. Energy consumption is more in TF-LEACH compared to LEACH-C as the cluster head communicates about malicious nodes in the network. Figure 8 shows that the number of data packets sent in network with TF-LEACHC is almost equal to original LEACHC as the malicious nodes are eliminated for further processing in the network. Figure 9 shows that the number of nodes alive in the network is 90 at simulation time 100, for TF-LEACHC, the reason is, it eliminates communication malicious nodes from the network. The final life time of network is almost same for all three types of the network.

The TF-LEACHC provides trust factor based secure communication for LEACHC protocol. The communication malicious nodes get detected and eliminated by the sink node for further processing. The data stealthy attackers are detected by cluster heads and eliminated by cluster heads for considering their data for aggregation.

5. CONCLUSION

The trust in wireless sensor network depends on the observed behavior of a node by its neighbor node. We propose a trust factor based centralized low energy adaptive cluster head (TF-LEACHC) protocol for trust based secure communication in the network. The simulation result shows that communication malicious node gets detected by 100%. The data stealthy attackers get detected by 100% for 10% attacker nodes and 50% for 30% attacker nodes. The reason is, the communication malicious node detection depends upon the behaviour of single malicious node. Where as detection of data stealthy attacker depends on the average value of data sensed by neighbour nodes. If there are more number of stealthy attacker nodes as neighbour, the calculated data average value will be in favour of malicious node. In such situations, false negative and false positive percentage increases in the network. The energy consumption in case of TF-LEACHC is more, compared to LEACH-C as the cluster head nodes maintains the list of communicate malicious node with sink nodes. As a future work, further improvement in detection of data stealthy attacks with more sophisticated methods are necessary.

6. REFERENCES

[1] Heinzelman, W, Chandrakasan, A, and Balakrishnan H. 2002, Energy-efficient communication protocols for wireless microsensor networks, Proceedings of the 33rd Hawaaian International Conference on Systems Science (HICSS), pp. 1-10.

[2] Yanli Yu, Keqiu Li, Wanlei Zhoui, Ping Li. 2012, Trust mechanisms in wireless sensor networks: Attacks analysis and countermeasures,"Journal of Network and Computer Applications, pp. 867-880.

[3] Fei Song, Baohua Zhao. 2008, Trust based LEACH protocol for wireless sensor networks, Proc. of the 2008 Second International Conference on Future Generation Communication and Networking, pp. 202-207.

[4] Mohammad Reza Rohbanian, Mohammad Rafi Kharazmi, Alireza Keshavarz-Haddad, Manije Keshtgary. Watchdog-LEACH: A new method based on LEACH protocol to secure clustered wireless sensor networks, http://arxiv.org/ftp/arxiv/papers/1310/1310.3637.pdf.

[5] Fenye Bao, Ing-ray Chen, Moonjeong Chang and Jin-hee Cho. 2011, Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection, Proc. of ACM Symposium on Applied Computing, pp 1732-1738.

[6] Geetha V, Pranesh V Kallapur, Sushma Tellajeera. 2012, Clustering in wireless sensor networks: Performance comparison of LEACH and LEACH-C protocols using NS2, Procedia Technology 4, pp 163-170.

[7] Meenakshi Tripathi, M.S. Gaur and V. Laxmi. 2013, Simulation of snooze attack in LEACH, AIRCCJ, Computer Science and Information Technology, CSCP, Volume 3,pp.393-399.doi:10.5121/csit.2013.3541.

[8] Shikha Magotra, Krishna Kumar. 2014, Detection of HELLO flood attack on LEACH protocol, Proc. of IEEE International Conference on Advanced Computing Conference(IACC), 2014, 193 - 198.

[9] Simerpreet Kaur, Md. Ataulla. 2014, Securing wireless sensor network from denial of sleep attack by isolating nodes, International Journal of Computer Applications, Vol 103, No-1, pp 29-33.

[10] Josang and R Ismail. 2002, The Beta reputation system, Proc. of the 15th Bled Electronic Commerce Conference. Bled, Slovenia.

[11] S Ganeriwal and M B Srivastava 2004, Reputation-based framework for high integrity sensor networks, Proc. of The 2nd ACM Workshop on Security of Ad-hoc and Sensor Networks Washington DC, USA.

[12] Network Simulator -2 (ns-2), http://www.isi.edu/nsnam/ns.