

Dynamic Trust Aware Systems in Wireless Sensor NetworksS.Rajasekar¹, D.Santha Kumar², K.Ashiq Irphan³¹²³Computer Science and Engineering, CKCET

Abstract —Sensor network is an adaptable technology for perceiving environmental criterions and hence finds its pivotal role in a wide range of applications. The applications range from mission critical like military or patient monitoring systems to home surveillance systems where the network may be prone to security attacks. The network is vulnerable to attack as it may be deployed in hostile environments. In addition it may be exposed to attacks due to the inherent feature of not incorporating security mechanisms into the nodes. Hence additional programs for security may be added in the network. One such scheme is making the network a trust ware system. The trust computation serves as a powerful tool in the detection of unexpected node behaviour. In this paper we propose a trust mechanism to determine the trustworthiness of the sensor node. Most of the existing trust aware systems are centralised and suffer from single head failure. In this paper we propose a dynamic and decentralized system.

Keywords-security, trust evaluation, wireless sensor network.

I. INTRODUCTION

Sensor network gains its popularity with the technological growth where it acts as an interface between the real world and digital data. Wireless sensor network can be defined as the self configured and infrastructure less network that cooperatively pass their data through network to the sink, where the aggregated data is observed and analyzed. Once the sensor nodes are deployed, they are responsible for self organizing infrastructure with single or multi-hop communication among them. They have larger flexibility in solving problems of different application domain like military, area monitoring, transport, environment sensing. Being deployed in the hostile and hazardous environment the sensor network can be easily compromised by adversary due to some constraints like battery lifetime, memory, energy, and its computing capability [1]. Hence it is a challenging and critical task to detect and isolate the faulty node in order to avoid being misled.

Attacks in the sensor network can be classified into two types namely passive and active attacks. Attacks that do not change the data during transmission are termed as passive and those which, attacks the data by modifying its contents, dropping the packets, acts selfish without detecting an event and saves its energy to launch attack on genuine nodes are termed to be passive attacks [2]. The adversary can even compromise the sensor devices without being detected of an attack. Therefore the sensor network should be robust against these attacks and its impact on other nodes should be minimized [3].

II. RELATED WORKS

The related works on trust computation specifies the reliability through the trust worthiness of the sensor nodes. The energy aware trust derivation scheme [4] employs the game theoretic approach called the trust derivation dilemma game (TDDG) which manages the overhead with the hop limit in the request with direct and indirect recommendation with well behaved and misbehaved activities for minimizing the energy utilization and latency of the network. However this may reduce communication involvement among the nodes upon reaching zero in hop limit. The trust management scheme for the unattended wireless sensor network [5], [6] detects outlier for pollution attacks by providing trusted data storage and trust generation through the geographical hash table with the trust similarity functions. The subjective logic technique employed here identifies trust fluctuations caused by environmental factors. The sensor nodes do not need to know the ID's of the storage nodes instead the hash function finds the location.

A lightweight trust decision making scheme [7], [8] is based on the node identities in the clustered WSN with the cancelling feedback between the cluster member and cluster head. Hence it significantly reduces the effect of malicious node. A self adaptive weighted method is defined from 0 to 1 for the trust aggregation at the cluster head level and it is a novel method for determining trust. An energy efficient trust based algorithm [9] concentrates on aggregation and energy. The nodes are selected based on reputation and trust. This is performed in order to find the best suited path from every node the link availability and the residual energy is taken into account. The short coming of energy efficient trust based algorithm is that it introduces delay in the network but it is compensated in terms of reliability and lifetime. Trust computation has been applied for data aggregation in [10] which evaluates the autonomous behavior of the sensor node with monitoring privileges. The cluster head assigns the weight value for the data from each of the sensor node and final data fusion process is executed where the cluster head transmit the fused result to the base station. Energy efficient clustering and routing in wireless mobile network [11], provides relocation of mobile nodes and energy efficient

clustering with weighted election probability and residual energy of node for electing cluster head and thereby it increase the network lifetime.

III. SYSTEM MODEL

3.1. Network Model

This model involves the network deployment where the sensor nodes are deployed at random and distance between the particular node and its neighboring nodes is calculated with the position of coordinates. The network model comprises of sensor node and verifiers and the interaction between them. The verifiers are normal sensor node with some additional capabilities. The nodes are grouped into cluster where the cluster head is elected explicitly through clustering algorithm in order to maintain the energy level of the cluster. The cluster head communicates with the base station

3.2. Security and attack

The sensor network is open and deployed in remote areas they are prone to security attacks. Sensor nodes are generally deployed in large numbers for monitoring various parameters and to obtain redundancy. But cost limits the security features to be incorporated into the sensor nodes.

3.3. Trust computation

The trust computation is a unified approach for specifying the security policies and relationship when nodes establish a network. Our trust evaluation scheme is devised to detect the misbehavior nodes with the parameters such as the request reply ratio, data forwarding and number of packets sent. In this paper the trust evaluation scheme is a weighted scheme where the weight value is assigned to the parameters instead of weightage to the nodes. Therefore it reflects a mutual relationship between highly trusted nodes by checking whether the given nodes behave in a trustworthy manner and maintains a reliable communications.

The trust computation is done by two ways as the direct trust and the indirect trust. The direct trust is based on the direct observation of node that participates in data transfer whereas the indirect trust is obtained from the recommendations of the verifiers. The event of trust calculation is done to obtain a safe and reliable path for inter and intra cluster communication.

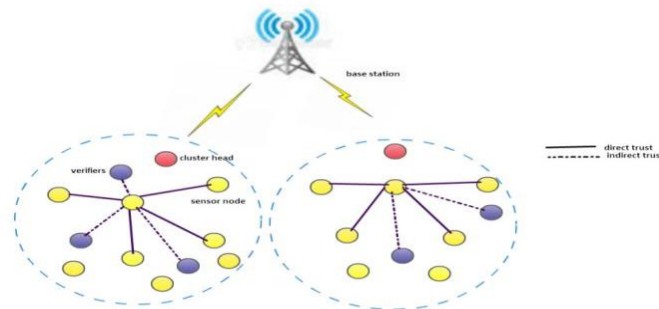


Figure 1. System Architecture

Notations	Meanings
$t_{mac(i)}$	Message authentication code
$t_{ct(i)}$	Cipher text
$t_{c(i)}$	Correctness of node
$t_{rr(i)}$	Receive reply ratio
$t_{po(i)}$	Base station remarks
$t_{fi(i)}$	Selfishness of node
$t_{df(i)}$	Data forwarding
$t_{uf(i)}$	Unwanted flooding
$t_{bm(i)}$	Behavior monitoring
w	Weight value for parameters
W	Overall Weight value for trust
T_D	Direct trust
T_I	Indirect trust
T	Overall trust

Table 1. Notations For Trust Evaluation

For the above mentioned parameters the weight value is assigned based on the priority for parameters. Hence the direct is calculated by

$$TD = tmac(i) * w1 + tct(i) * w2 + tc(i) * w3 + trr(i) * w4 + tpo(i) * w5 + tti(i) * w6$$

$$TI = (\sum t) / m$$

Where

$$tm = tdf * w1 + tuf * w2 + tbm * w3.$$

$$\sum t = tm1 + tm2 + \dots + tmn$$

The total trust value for the nodes is calculated with the combination of direct and indirect trust evaluation.

$$T = T_d * W_1 + T_i * W_2$$

Where

$$W_1 + W_2 = 1$$

When nodes trust value is less than 0.5 it is considered to be a malicious node provided we assume that at least 50 percentile of the nodes are genuine nodes in a network.

IV. SIMULATION RESULTS

The proposed work is implemented with the network simulator (NS2) to detect the faulty node from the network and by improving the performance of the system.

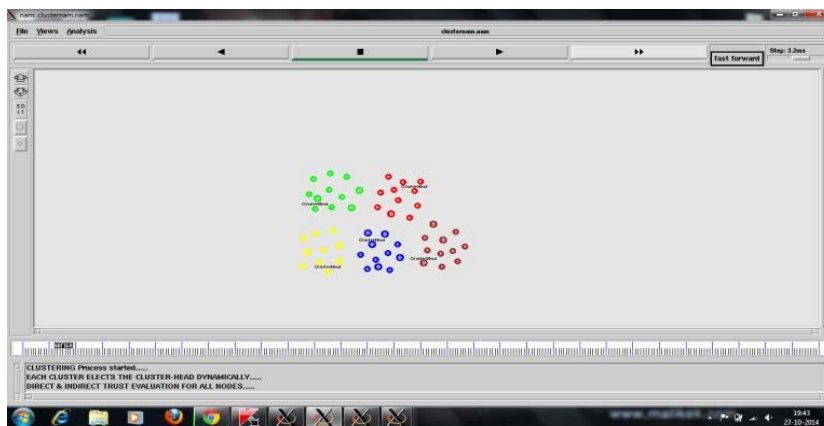


Figure.2. Initialization of the sensor network

Figure.2 represents the initialization of the sensor network wherein the nodes are deployed in random with clustering mechanism.

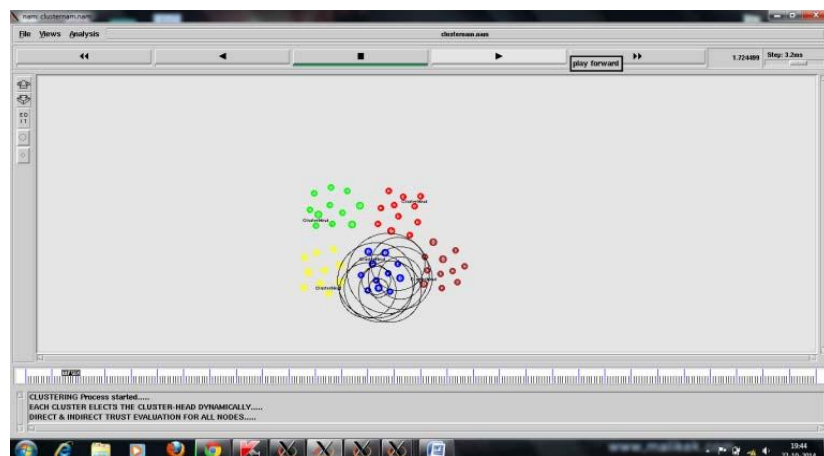
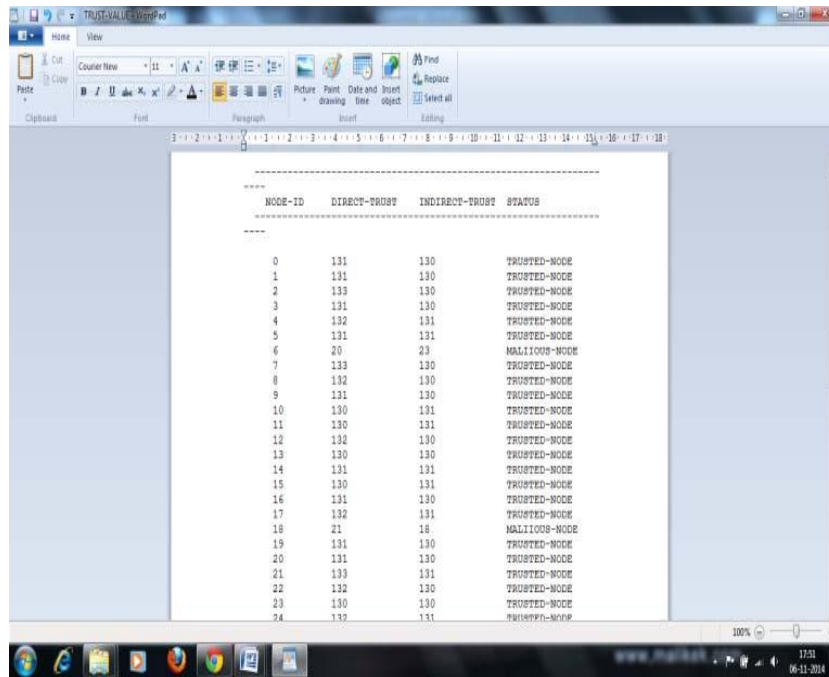


Figure.3. Direct and Indirect trust computation

Figure.3 represents the direct and indirect trust simulation process for each and every node from our proposed trust generation mechanism



NODE-ID	DIRECT-TRUST	INDIRECT-TRUST	STATUS
0	131	130	TRUSTED-NODE
1	131	130	TRUSTED-NODE
2	133	130	TRUSTED-NODE
3	131	130	TRUSTED-NODE
4	132	131	TRUSTED-NODE
5	131	131	TRUSTED-NODE
6	20	23	MALICIOUS-NODE
7	133	130	TRUSTED-NODE
8	132	130	TRUSTED-NODE
9	131	130	TRUSTED-NODE
10	130	131	TRUSTED-NODE
11	130	131	TRUSTED-NODE
12	132	130	TRUSTED-NODE
13	130	130	TRUSTED-NODE
14	131	131	TRUSTED-NODE
15	130	131	TRUSTED-NODE
16	131	130	TRUSTED-NODE
17	132	131	TRUSTED-NODE
18	21	18	MALICIOUS-NODE
19	131	130	TRUSTED-NODE
20	131	130	TRUSTED-NODE
21	133	131	TRUSTED-NODE
22	132	130	TRUSTED-NODE
23	130	130	TRUSTED-NODE
24	132	131	TRUSTED-NODE

Figure.4. Generated trust values of the nodes



Figure. 5.Performance Evaluation

Fig.5 represents the performance evaluation for the proposed system (a) throughput (b) routing overhead (c) packet delivery ratio (d) network life time.

The above performance evaluation is based on comparing the existing system with the proposed system. The throughput of the existing method attains a steady state after 25ms when compared with the proposed system reaches its steady state in the initial stage of 5ms. The routing overhead incurred in existing system is lesser when compared to the proposed system. The packet delivery ratio and network life time with respect to time of the proposed system shows better performance. The above performance evaluation results signifies that our proposed system is efficient with increased throughput, packet delivery ratio and network lifetime. The proposed system incurs routing overhead, because of the need for trust computations and communication required to transmit the trust. After trust computation, the malicious node or nodes with same id are identified and it is revoked from the network. Hence the routing overhead is justified with the security and considered to be a trade off for node security. The proposed system prevents malicious node attacks and the data in the network is transferred through a secured path.

V. CONCLUSION

Our proposed system provides the trust evaluation for each node in a dynamic and decentralised method to find out whether a node is genuine and enhance the sensor network security. Our future work is to examine trust evaluation with localization in order to avoid replication attack on nodes with malicious node monitoring with minimal communication cost

REFERENCES

- [1] Raja Waseem Anwar, Majid Bakhtiari, Anazida Zainal, Abdul Hanan Abdullah and Kashif Naseer Qureshi, "Security issues and attacks in wireless sensor network," *World Applied Sciences Journal*, vol. 30, no.10, pp.1224-1227, 2014.
- [2] V.Umarani and Soma Sundaram, "Survey of various trust models and their behavior in wireless sensor network," *International Journal of Emerging Technology and Advanced Engineering*, vol. 3, no. 10, pp. 180-188, October 2013.
- [3] J.H.Cho, A.Swami and I.R.Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Communications Survey and Tutorials*, vol. 13, no. 4, pp. 562-583, 2011.
- [4] Junqi Duan, Deyum Gao, Dong Yang, Chuan Heng Foh and Hsiao Hwa Chen, "An energy aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 58-69, February 2014.
- [5] Yi Ren, Vladimir I.Zadorozhny, Vladimir A.Oleshchuk and Frank Y.Li, "A novel approach to trust management in unattended wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 13, no. 7, pp. 1409-1423, July 2014.
- [6] Y.Ren, V.I.Zadorozhny, V.Oleshchuk and F.Y.Li, "An efficient robust and scalable trust management scheme for unattended wireless sensor networks," in *Proc. IEEE International Conference on Mobile Data Management*, Bengaluru, India, July 2012.
- [7] Xiaoyong Li, Feng Zhou and Junping Du, "A lightweight and dependable trust system for clustered wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 6, pp. 924-935, June 2013.
- [8] G.V.Crosby and N.Pissinou, "Cluster based reputation and trust for wireless sensor networks," in *Proc. International Conference on Consumer Communications and Networking*, Las Vegas, NV, USA, 2007.
- [9] Z.Taghikhaki, N.Meratnia and P.J.M.Havinga, "Energy efficient trust based aggregation in wireless sensor networks," in *Proc. IEEE International Workshop on Wireless Sensor Actuator and Robot Networks (WiSARN 2011)*, pp. 584-589, April 2011.
- [10] Zhou Jianming, Liu Fan and Lu Qiuyuan, "Data fusion based on node trust evaluation in wireless sensor networks," *Journal of Sensors*, vol. 1, pp. 1-7, July 2014.
- [11] S.Getsy, R.Sara Kalaiaresi, S.Neelavathy Pari and D. Sridharan, "Energy efficient clustering and routing in wireless mobile network," *International Journal of wireless and Mobile Networks (IJWMN)*, vol. 2, no. 4, pp. 106-114, November 2010.