Improved Trust System for Clustered Wireless Sensor Network

S. Mahitha and N. Shanmugapriya

Abstract--- In wireless sensor network the resource efficiency and reliability of a trust system are the most basic supplies. Due to the low reliability and high overhead the developed existing trust systems for wireless sensor networks are unable of satisfying these supplies. Therefore there is need to propose a lightweight and reliable trust system which can efficiently decrease the networking consumption while malicious, selfish and faulty cluster heads and also exceeds the limitations of traditional weighting methods for trust factors in which weights are allocated subjectively and also insist less communication overhead and memory. In this work, Improved Trust System (ITS) is proposed for clustered WSNs. In the ITS protocol, the trust system defines the tasks of the nodes as sensing, aggregating and routing, and evaluating the trustworthiness of each task based on first-hand and second-hand information. Here the trust metrics such as energy, link availability, along with Per-hop Packet Pair Delay are used. The residual energy, link availability between nodes and Per-hop Packet Pair Delay ie., calculation of the time required to reach the destination and to receive the acknowledgement of receipt sent by the sending node must be taken into consideration and combined with the reputation and trust system to keep the network secure, reliable, and energy-efficient. Theory as well as simulation results show that ITS demands less memory and communication overhead as compared with other typical trust systems and is more suitable for clustered WSNs.

Keywords--- Clustered Wireless Sensor Network, Improved Trust System, Energy, Link Availability, Per-hop Packet Pair Delay

I. INTRODUCTION

Wireless sensor networks (WSNs) consist of many resource-constrained sensor nodes. Due to low cost, sensor nodes have poor reliability and are prone to node compromise and node failures. Traditional security mechanisms, such as authentication and cryptography, cannot secure the network against internal attacks launched by captured nodes. E.g, an adversary can place several intruder nodes or compromise sensor nodes in the network to disrupt the network's normal operation by sending false sensing data or falsifying delivered results. The false messages can mislead users to make a wrong decision. If malicious nodes injecting these false data into the network have been authenticated as legal nodes, conventional security mechanisms have no ability to differentiate those from legal nodes. Trust management, which has been proved as an effective approach to assessing trustworthiness of sensor nodes [1], becomes essential to the robust operation of sensor networks. Trust management techniques have been widely used in various fields, from Internet, P2P networks to ad−hoc networks, such as eBay [2], RFSN [3], TEFDN [4], etc.

In the past decade, a large number of trust management schemes in WSNs have been proposed to identify malicious nodes. Although trust management of sensor networks has made a lot of progress, existing Trust Management Systems (TMSs) are difficult to distinguishing between normal and malicious nodes effectively because of sensor nodes being cheap, unreliable, and easily impacted by environmental noise. When sensor nodes were deployed in complicated environment, normal nodes were usually judged to be malicious nodes since packet loss and packet forwarding

S. Mahitha, M.Phil Scholar, Dr. SNS Rajalakshmi College of Arts and Science. E-mail:mahitha.loganathan23@gmail.com

N. Shanmugapriya, Asst. Prof, Department of Computer Applications(MCA), Dr. SNS Rajalakshmi College of Arts and Science

failure often occurred in the complicated environments. If too many normal nodes were judged to be malicious nodes, it will eventually lead to network paralysis.

How to improve the success ratio of distinguishing malicious nodes in complex environments has become an urgent problem in the trust management field of WSNs. This paper considers that Improved Trust System (ITS) for clustered WSNs. The main contribution of this ITS is that it offers a cluster based trust rating model to detect the compromised sensor nodes. It develops a way to calculate the trust of a cluster. In the ITS protocol, the reputation and trust system defines the tasks of the nodes as sensing, aggregating and routing, and evaluating the trustworthiness of each task based on first-hand and second-hand information. Here the trust metrics such as energy, link availability, along with Per-hop Packet Pair Delay. The residual energy, link availability between nodes and Per-hop Packet Pair Delay ie., calculation of the time required to reach the destination and to receive the acknowledgement of receipt sent by the sending node must be taken into consideration and combined with the reputation and trust system to keep the network secure, reliable, and energy-efficient.

The rest of this paper is organized as follows. Some related works are reviewed in Section II. The proposed Per-hop Packet Pair Delay based trust model for short-term trust value estimation of nodes is presented in Section III. Section IV compares the proposed ITS with LDTS: A Lightweight and Dependable Trust System for Clustered Wireless Sensor Networks, and shows simulation results. The paper ends with conclusion in section V.

II. RELATED WORK

Trust has been studied in a variety of networks and applications. A large number of trust models have been proposed in social networking. In this section, existing works that are somewhat related to proposed research is reviewed.

Kim, T. K., & Seo, H. S. et al [5] formulated the trust model using fuzzy logic for the safe communication between source and destination node in wireless sensor network. We focused on the trustworthy of sensor node which participating the wireless network. If the sensor node has high trust value, other node can trust the sensor node and sending and receiving a data safely with it.

Huang, L., Li, L., et al [6] explained the resource constraints of wireless sensor network make it easy to attack and hard to protect. Although carefully designed cryptography and authentication help to make WSN securer, they are not good at dealing with compromised node and ageing node, whose misbehavior may impair the function of WSN. Behavior-based trust mechanism, which is a variant of reputation-based trust in eCommerce, can be used to address this problem. The framework and related techniques of behavior-based trust are discussed in this paper.

Crosby, G. V., Pissinou, N et al [7] proposed mechanism reduces the likelihood of compromised and or malicious nodes from being selected as cluster heads. Our premise is that while individual nodes may still be prone to attack, a significant vulnerability is addressed if we prevent the election of compromised cluster heads. We do not seek a 'cure for all solution' rather we introduce a framework and a mechanism to address a potentially significant security breach. We performed an evaluation of our approach and the power consumption of our model, by simulations. The results indicate clear advantages of our approach in preventing the election of untrustworthy cluster heads

Shaikh et.al [8] proposes a light weight Group Based Trust Management Scheme (GTMS) for clustered WSN. GTMS contain a single trust value for each cluster. All Sensor nodes in a cluster calculate individual trust values for all group members to the cluster head. Cluster head aggregates and evaluates the trust values of each node and forwards the calculated value to the base station as well as detects the malicious node in a cluster. Depending on the trust values of all the clusters, the base station assigns the one out of the three possible states, namely trusted, untrusted and uncertain to the whole group. This scheme is very simple and flexible and does not require large memory of data and complex computations at sensor nodes. The scheme provides protection against malicious, selfish and faulty nodes. The main limitation of the GTMS scheme is that use of some unrealistic assumption for protecting the trust values of clusters from attacks.

Atakli, I. M., Hu, H., et al [9] Deployed in a hostile environment, individual nodes of a wireless sensor network (WSN) could be easily compromised by the adversary due to the constraints such as limited battery lifetime, memory space and computing capability. It is critical to detect and isolate the compromised nodes in order to avoid being misled by the falsified information injected by the adversary through compromised nodes. However, it is challenging to secure the flat topology networks efficiently because of the poor scalability and high communication overhead. On top of a hierarchical WSN architecture, in this paper we proposed a novel scheme based on weighted-trust evaluation to detect malicious nodes. The hierarchical network can reduce the communication overhead between sensor nodes by utilizing clustered topology. Through intensive simulation, we verified the correctness and efficiency of our detection scheme.

Mármol, F. G., & Pérez, G. wt al [10] explained Wireless Sensor Networks (WSNs) are becoming more and more spread and both industry and academia are focusing their research efforts in order to improve their applications. One of the first issues to solve in order to achieve that expected improvement is to assure a minimum level of security in such a restrictive environment. Even more, ensuring confidence between every pair of interacting nodes is a critical issue in this kind of networks. Under these conditions we present in this paper a bio-inspired trust and reputation model, called BTRM-WSN, based on ant colony systems aiming at providing trust and reputation in WSNs.

Boukerch, A., Xu, L., & El-Khatib et al [11] Trust and reputation have been recently suggested as an effective security mechanism for open environments such as the Internet, and considerable research has been done on modeling and managing trust and reputation. Using the trust and reputation management scheme to secure wireless sensor networks (WSNs) requires paying close attention to the incurred bandwidth and delay overhead, which have thus far been overlooked by most research work. In this paper, we propose a novel Agent-Based Trust and Reputation Management Scheme (ATRM) for wireless sensor networks. The objective of the scheme is to manage trust and reputation locally with minimal overhead in terms of extra messages and time delay.

Crosby, G. V., & Pissinou, N. et al [12] described a reputation based trust framework with a mechanism for the election of trustworthy cluster heads. Our trust framework is design in the context of a cluster based network model with nodes that have unique local IDs. We assess our model based on power consumption and its ability to prevent compromised nodes from becoming cluster heads. Our approach decreases the likelihood of malicious or compromised nodes from becoming cluster heads.

III. PROPOSED METHOD

In this section, the improved trust management system is proposed to solve the security and energy problem in sensor nodes and evaluated the trust values in clustered wireless sensor network are explained.

System Model

In this paper, the hierarchal cluster architecture was used to construct WSNs composed of sensor nodes that were densely deployed in clusters. It was assumed that the operation of each cluster was relatively independent and that very few, if any; non overlapping areas would be sensed between the clusters. Hence, the reputation and trust of the sensor nodes are evaluated only by the nodes in their own cluster. A watchdog mechanism is used to monitor and detect the actions of target nodes, and those actions are characterized as cooperative or non cooperative; judgments are made concerning whether the action of the nodes are right or not. Thus, the reputation and trust system is responsible for maintaining the reputation and trust of a node, and this duty includes many tasks. The system updates reputation information based on new observations made by the improved watchdog mechanism and creates new evaluations of the trustworthiness of the nodes.

Each cluster has a cluster head called an aggregator, which is in charge of a certain number of sensor nodes and has the capability of performing the data-aggregation operation. Aggregators are utilized to process received data from children nodes and transmit the aggregated results to base station. Sensor nodes, with the exception of the aggregator, sense the data, monitor the activities of other nodes, exchange observations with neighboring nodes, evaluate the trustworthiness of the nodes, and transmit data and observations to the aggregator. When the sensor nodes report their readings to the aggregators, the messages are encrypted and decrypted by pair wise keys that are generated and that are possessed only by the two communicating parties through their negotiation. In addition, the aggregators, namely, the cluster heads that are in the hierarchal cluster architecture, are not maintained for a long term and dynamically changing, because, when the system is running, adversaries can follow the aggregators more and more closely, so security problems associated with those aggregators will increase. In addition, the energy consumption of those aggregators increases rapidly and significantly when they remain unchanged for extended periods. Thus, to solve the security and energy problem, sensor nodes in the cluster must be reselected dynamically as aggregators at intervals.

Reputation and Trust Computation

In the proposed Improved Trust System (ITS) protocol, the reputation and trust system defines the tasks of the nodes as sensing, aggregating and routing, and evaluating the trustworthiness of each task based on first-hand and second-hand information. Here the trust metrics such as energy, link availability, along with Per-hop Packet Pair Delay. The residual energy, link availability between nodes and Per-hop Packet Pair Delay ie., calculation of the time required to reach the destination and to receive the acknowledgement of receipt sent by the sending node must be taken into consideration and combined with the reputation and trust system to keep the network secure, reliable, and energy-efficient.

Sensor nodes in the routing path, in addition to their sensing task, must relay data towards the aggregators and base station. Sensor nodes and aggregators record their residual energy and exchange this information with neighboring nodes. Then, the nodes can use the energy information to determine the link availability between them. Thus, the aggregators also can obtain the status of the energy levels of the nodes along with time taken for packet to reach destination or ack to reach to source node in their cluster and identify the best nodes for forwarding data to the base station. The values are stored as table format and exchanged simultaneously. When they are received, there are two advantages in the data-aggregation operation; that is, (1) in each cluster, nodes can select the best aggregator of the cluster in a certain time period according to reputation and energy information. The selection requires the consensus of all the nodes' points and is determined based on the equilibrium of reputation and energy, and (2) after the aggregation is completed in each cluster, then results of the aggregation are transmitted to the base station along the routing path. Combining reputation and energy information could confirm link availability between nodes and identify a better path from each aggregator to the base station. It is also useful to select the best path from the sensor nodes to their clusters' aggregators.

Trust Calculation

The parameter N_{ET} is defined below to represent a node's combined information of reputation and energy. Calculating the parameter N_{ET} helps the system identify the best aggregator and routing nodes in each cluster:

$$N_{ET} = \frac{E \times T}{Init - E \times Init - T}$$

Where E is a energy for each nodes and T reputation of each node. Init is initial value of both energy and reputation values for particular nodes. Here reputation is considered as time taken for delivery packets or delivery of acknowledgement. The destination node calculates how long it will take both packets to reach the destination from the source (delays) and sends back the information to the sender.

Link availability between nodes

$$L_{AB} = \frac{Init - T_{AB} \cdot Init - E_B}{T_{AB} \cdot E_B}$$

Where T_{AB} represents the reputation of node *B* evaluated by node *A*, E_B is the residual energy of node *B*.

Assume that there are *p* two-hop nodes with link availability in the routing path between *i* and *j*, each with the middle nodes *s l* (1 < *l* < *p*), and denote (*i*, *j*) as the link availability of nodes between *i* and *j*. The whole link availability between *i* and *j* is denoted as Link (*i*, *j*):

$$Link(i,j) = L(i,j) + \mathop{}_{l=1}^{p} \min(L(i,s_l), L(s_l,j))$$

The network uses residual energy and link availability to reselect the aggregators and routing paths every T_x time period. It is possible that some links between nodes will fail during the time period. So this operation is done each T_x time period, and the new information of new aggregators and new upstream nodes in the cluster is shared and recorded.

Proposed Algorithm
Step 1: initialize the nodes in network
Step 2: form the clusters based on the distance and initial energy of the node
Step 3: cluster head is selected
Step 4: select the source node in cluster
Step 5: source initializes the request for collecting the first and second information about particular to neighboring nodes in two ways such as on demand and broadcasting
Step 6: The on demand procedure takes place when node N_i requests that neighboring nodes exchange observation tables with it and uses the observations to evaluate the reputation of N_j.
Step 7: Broadcasting refers to the case in which the nodes broadcast their observation tables for a certain time period. (Here tables represent the first hand and second information ie., energy, link availability and path delay parametric value stored in the table format)
Step 8: evaluation of the trust for node N_j in N_i

When the node N_i is detecting and monitoring the sensing task of nodeN_j, the numbers of behaviors and misbehaviors of node N_j as judged by node N_i are recorded as $\alpha_{i,j}^{new}$ and $\beta_{i,j}^{new}$, respectively. Reputation value and trust for the sensing task of node N_j are represented by $R_{i,j}^{sensing}, j$ and $T_{i,j}^{sensing}$, respectively. The formula of reputation and trust calculation is

$$R_{i,j}^{sensin\ g} = Beta\left(\alpha_{i,j}^{new} + 1, \beta_{i,j}^{new} + 1\right)$$

$$= \frac{\Gamma\left(\alpha_{i,j}^{new} + 1 + \beta_{i,j}^{new} + 1\right)}{\Gamma\left(\alpha_{i,j}^{new} + 1\right) \cdot \Gamma\left(\beta_{i,j}^{new} + 1\right)} \varphi^{\left(\alpha_{i,j}^{new} + 1\right) - 1} (1 - \varphi)^{\left(\beta_{i,j}^{new} + 1\right)}$$

$$T_{i,j}^{sensing} = E\left(R_{i,j}^{sensing} = \frac{\alpha_{i,j}^{new} + 1}{\alpha_{i,j}^{new} + \beta_{i,j}^{new} + 2}\right.$$

The parameters $\alpha_{i,j}^{new}$ and $\beta_{i,j}^{new}$ are the new numbers of correct and false actions of node N_j calculated by first-hand and second-hand information. The process of integrating first-hand and second-hand information into an overall reputation was proposed, and it is shown below:

$$\alpha_{i,j}^{new} = p * \alpha_{i,j}^{now} + m_{i,j} + \sum_{k \in N} R\left(m_{k,j}\right)$$

$$\beta_{i,j}^{new} = p * \beta_{i,j}^{now} + n_{i,j} + \sum_{k \in N} R\left(n_{k,j}\right)$$

Where parameters $\alpha_{i,j}^{now}$ and $\beta_{i,j}^{now}$ are the last observations about correct and bad actions of N_j in the observation table, respectively, and $m_{i,j}$ and $n_{i,j}$ represent the number of recent observations of correct and bad sensing actions, respectively. Old feedback cannot always work effectively for the new reputation and trust rating during the operation, so the old observations are less important than most recent observations, and they will be eliminated gradually. Therefore, the elimination parameter$p$ < 1is introduced to achieve the characteristic of last observations described above. In addition, second-hand information is exchanged between node N_i and N_k $(k = 1, 2, \ldots, n)$, and the observed numbers of correct and bad behaviors are expressed as $R(m_{k,j})$ and $R(n_{k,j})$ $(k = 1, 2, \ldots, n)$, respectively. Second-hand information for correct and bad actions is defined in [20] and is shown below:

$$R(m_{k,j}) = \frac{2 * \alpha_{i,k}^{now} \ * m_{k,j}}{\left(\beta_{i,k}^{now} \ + 2\right) * \left(m_{k,j} + n_{k,j} + 2\right) * \left(2 * \alpha_{i,k}^{now}\right.}$$

$$R(n_{k,j}) = \frac{2 * \beta_{i,k}^{now} \ * n_{k,j}}{\left(\beta_{i,k}^{now} \ + 2\right) * \left(m_{k,j} + n_{k,j} + 2\right) * \left(2 * \alpha_{i,k}^{now}\right.}$$

The WSN provides an intelligent platform to gather and analyze data without human intervention. As a result, WSNs have a wide range of applications such as military applications, to detect and track hostile objects in a battle field or in environmental research applications, to monitor a disaster as seismic tremor, a tornado or a flood or for industrial applications, to guide and diagnose robots or machines in a factory or for educational applications, to monitor developmental childhood or to create a problemsolving environment. Wireless sensors and sensor networks, pervasive computing, and artificial intelligence research together have built the interdisciplinary concept of Ambient Intelligence (AmI) in order to overcome the challenges we face in everyday life. One of the major challenges of the world for the last decades has been the continuous elderly population increase in the developed countries. Population Reference Bureau forecasts that in the next 20 years, the 65-and-over population in the developed countries will be nearly 20% of the overall population. Hence the need of delivering quality care to a rapidly growing population of elderly while reducing the healthcare costs is an important issue. One promising application in that area is the integration of sensing and consumer electronics technologies which would allow people to be constantly monitored. In-home pervasive networks may assist residents and their caregivers by providing continuous medical monitoring, memory enhancement, control of home appliances, medical data access, and emergency communication. Constant monitoring will increase early detection of emergency conditions and diseases for at risk patients and also provide wide range of healthcare services for people with various degrees of cognitive and physical disabilities. Not only the elderly and chronically ill but also the families in which both parents have to work will derive benefit from these systems for delivering high-quality care services for their babies and little children.

IV. Results and Discussion

In the ITS simulator, three kinds of nodes exist based on their identities such as a CM, as a CH, and as a BS. A CM or a CH can be a collaborator or a rater toward other nodes. The behavior of a CM as a collaborator can be one of two types: Good CM (GCM) and Bad CM (BCM). GCMs will provide successful interaction for the requested messages, whereas BCMs will provide an unsuccessful interaction. The behavior of a CM as a rater can be one of two types: Honest CM (HCM) and Malicious CM (MCM). An HCM always gives the appropriate rating for any CM, whereas an MCM always gives a random rating between 0 and 10 for other CMs. Similar to a CM, a GCH always provide successful interaction, whereas a BCH provide an unsuccessful interaction. An HCH always gives an appropriate rating, whereas an MCH always gives random rating between 0 and 10.

ITS protocol works with two topologies: the inter cluster (CH-to-CH) topology, where distributed trust management is used, and intra cluster (CM-to-CM) topology, where the centralized trust management approach is employed. We also find that different calculation mechanisms are employed for intra cluster and inter cluster trust evaluations. According to these characteristics of ITS, in this simulator, we separately evaluate the performance of ITS based on intra cluster and inter cluster cases. This approach will not affect the results of performance evaluation and will greatly reduce the complexity of the simulator.

Performance Evaluation

Overhead Evaluation and Comparison

The increasing number of CMs in a cluster, the CM-to-CM communication overhead of GTMS rapidly increased according to an exponential curve. However, the CM-to-CM communication overhead of LDTS slowly increased with the increasing number of CMs. But the CM-to-CM communication overhead of ITS slowly increased with the increasing number of CMs compare than LDTS. This trust calculation mechanism in ITS can greatly reduce communication overhead.

Fig. 1 shows the comparison results of the CH-to-CH communication overhead between ITS and existing LDTS. ITS and LDTS have a relatively close network overhead as the network size increases, which indicates that both LDTS and ITS are suitable for large-scale clustered WSNs. However, by comprehensively analyzing the results in Figs.1, ITS is more suitable for large-scale clustered WSNs with a large size of clusters, thus outperforming LDTS.

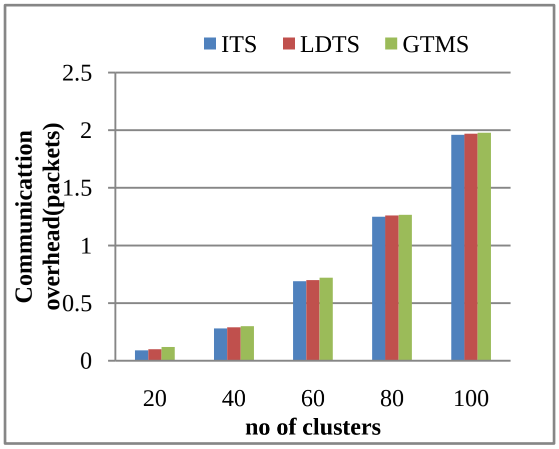

Fig. 1: CH-to-CH Communication Overhead in a Network

Fig. 2 shows the comparison results of average storage overhead at each CM in a cluster. With the increasing number of CMs in a cluster, the average storage overhead of GTMS gradually increased according to a linear curve. However, the average storage overhead of LDTS was less than a third of that of GTMS and slowly increased with the increasing number of CMs. But the proposed ITS was more less overhead than the existing LDTS and GTMS.

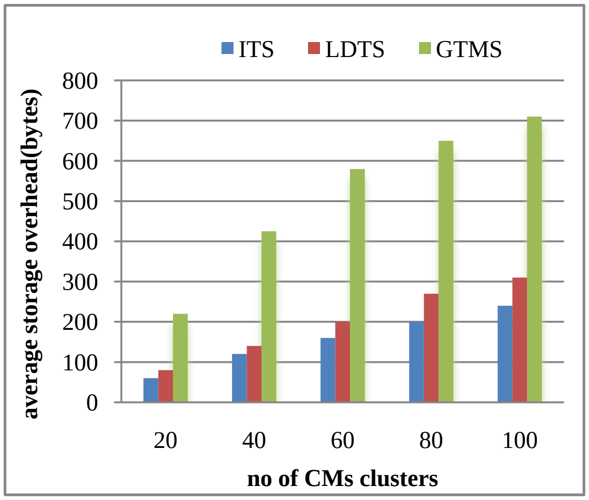

Fig. 2: Average Storage Overhead at Each CM in a Cluster

Throughput Evaluation

Throughput is defined as the total number of packets delivered over the total simulation time.

Mathematically, it can be defined as:

$$\text{Throughput} = N/1000$$

Where N is the number of bits received successfully by all destinations.

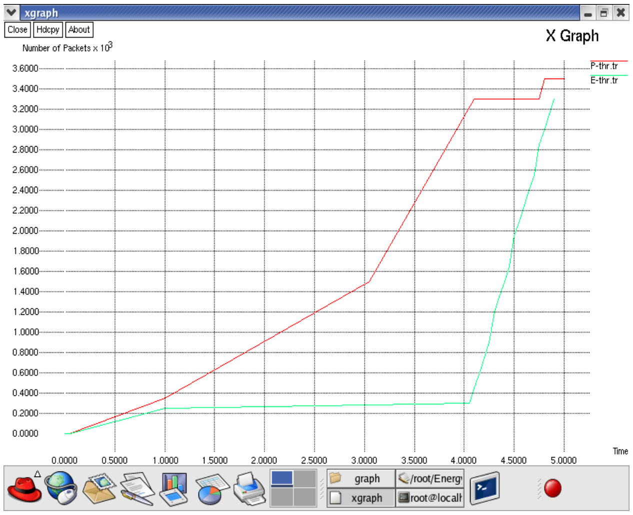

Fig. 3: Throughput Comparison

Fig.3 shows the throughput comparison of the proposed ITS protocol approach and the existing LDTS. It is noted that the proposed ITS protocol attains higher throughput when compared with the existing LDTS protocol. The reason is that, the probability to meet the desired event data in a short hop count is very high in such a way.

Packet Delivery Ratio

Fig.4. shows that the below graph is plotted across the number of nodes and the Packet Delivery Ratio (PDR). Normally the value of PDR will get increased when compared with the existing methods. In this graph, it shows that the packet delivery ratio increased for the proposed ITS protocol model since it stores, the best individuals in the memory when compared to the existing LDTS.

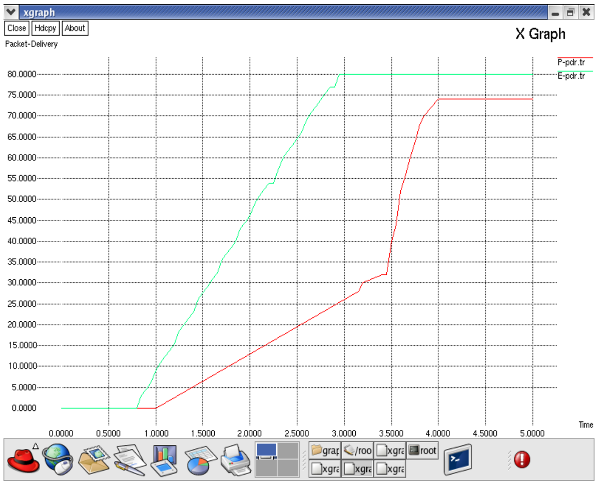

Fig. 4: Packet Delivery Ratio vs. No of Clusters

Energy Efficiency Comparison

Energy efficiency is defined to be the ratio of the amount of energy consumed per successfully packet delivered in network.

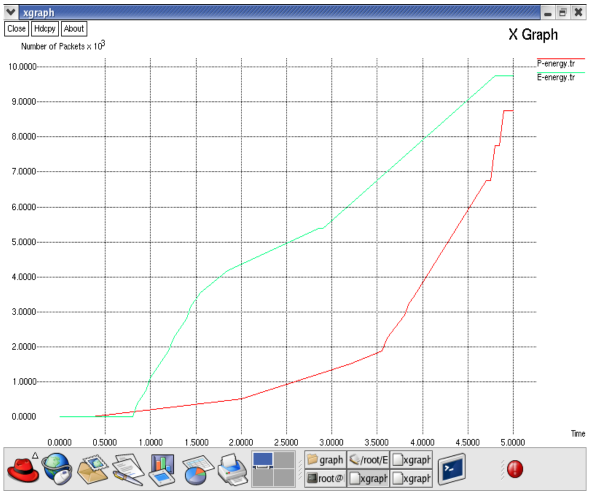

Fig. 5: Energy Efficiency Comparison Results

Figure5 shows that the proposed and existing comparison results with its respective energy consumption. From the figure it is obvious that the proposed ITS is consumes less energy than the existing system LDTS. When the time increases the energy consumption of the proposed system is decreases than the existing system**.**

Average Delay Comparison

Average delay is described as the average time taken for a packet to reach destination from the source.

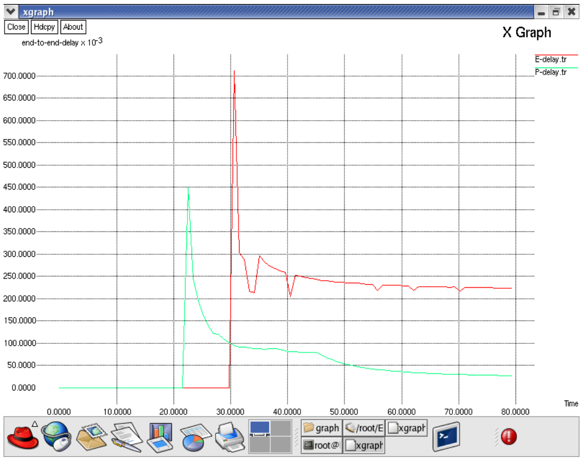

Fig. 6: Average Delay Comparison Results

Figure 6 shows that the average delay comparison results of the existing and the proposed system. The figure shows that the proposed ITS deliver significant results that have a lesser average delay in comparison with existing system LDTS. When the time increases the average delay of the proposed system is decreases than the existing system linearly.

V. Conclusion

The notion of trust, as used in different research areas like trusted computing, trusted platforms, trusted code and trust management, has received various interpretations. Throughout this work, we use the notion of trust as the quantified belief by a trust or with respect to the competence, trust, security and dependability of a trustee within a specified context''. In this work, ITS for clustered WSNs is proposed. In the proposed Improved Trust System (ITS) protocol, the reputation and trust system defines the tasks of the nodes as sensing, aggregating and routing, and evaluating the trustworthiness of each task based on first-hand and second-hand information. Here the trust metrics such as energy, link availability, along with Per-hop Packet Pair Delay. The residual energy, link availability between nodes and Per-hop Packet Pair Delay ie., calculation of the time required to reach the destination and to receive the acknowledgement of receipt sent by the sending node must be taken into consideration and combined with the reputation and trust system to keep the network secure, reliable, and energy-efficient. Theory as well as simulation results show that ITS demands less memory and communication overhead as compared with other typical trust systems and is more suitable for clustered WSNs. There are several future research directions, including (a) devising and validating a decentralized trust management scheme for autonomous WSNs without base stations; (b) investigating the impact of the cluster size and the trust update interval to the protocol performance and lifetime of a given WSN; and (c) investigating the feasibility of applying hierarchical trust management to more dynamic networks such as mobile WSNs, mobile cyber physical systems, or MANETs.

Reference

[1] M. Blaze, J. Feigenbaum, and J. Lacy, “Decentralized trust management.” IEEE Security and Privacy, Oakland, CA, May. 1996.

[2] P. Resnick, R. Zeckhauser, “Trust among strangers in internet transactions: Empirical analysis of eBay’s reputation system,” Emerald Group, Vol. 11, No. 1, Pp.127-157, Apr. 2002.

[3] S. Ganeriwal, M. Srivastava, “Reputation-based framework for high integrity sensor networks,” ACM S Network, New York, USA, 2004.

[4] Y. L. Sun, Z. Han, W. Yu, and K. J. R. Liu, “A trust evaluation framework in distributed networks: vulnerability analysis and defense against attacks,” IEEE Infocom, Vol. 6, Pp. 1-13, 2006.

[5] Kim, T. K., & Seo, H. S. (2008). A trust model using fuzzy logic in wireless sensor network. World academy of science, engineering and technology, 42(6), 63-66.

[6] Huang, L., Li, L., & Tan, Q. (2006). Behavior-based trust in wireless sensor network. In Advanced Web and Network Technologies, and Applications (pp. 214-223). Springer Berlin Heidelberg.

[7] Crosby, G. V., Pissinou, N., & Gadze, J. (2006, April). A framework for trust-based cluster head election in wireless sensor networks. In Dependability and Security in Sensor Networks and Systems, 2006. DSSNS 2006. Second IEEE Workshop on (pp. 10-pp). IEEE.

[8] Shaikh, R. A., Jameel, H., d'Auriol, B. J., Lee, H., Lee, S., & Song, Y. J. (2009). Group-based trust management scheme for clustered wireless sensor networks. Parallel and Distributed Systems, IEEE Transactions on, 20(11), 1698-1712.

[9] Atakli, I. M., Hu, H., Chen, Y., Ku, W. S., & Su, Z. (2008, April). Malicious node detection in wireless sensor networks using weighted trust evaluation. In Proceedings of the 2008 Spring simulation multiconference (pp. 836-843). Society for Computer Simulation International.

[10] Mármol, F. G., & Pérez, G. M. (2011). Providing trust in wireless sensor networks using a bio-inspired technique. Telecommunication systems, 46(2), 163-180.

[11] Boukerch, A., Xu, L., & El-Khatib, K. (2007). Trust-based security for wireless ad hoc and sensor networks. Computer Communications, 30(11), 2413-2427.

[12] Crosby, G. V., & Pissinou, N. (2007, January). Cluster-based reputation and trust for wireless sensor networks. In Consumer Communications and Networking Conference (pp. 604-608).