Improved Light Weight Dependable Trust Management System (LDTs) in Wireless Sensor Networks

S. Jegadeeshwari and R. Balakrishnan

Abstract--- Wireless sensor network (WSN) contains thousands of sensor nodes with less memory and low power devices. The major challenge faced by wireless sensor networks is security. Because of dynamic and collaborative nature of sensor networks the connected sensor devices makes the network unusable. To solve this issue, a trust model is required to identify malicious, selfish and compromised nodes. However, existing trust systems developed for WSNs are incapable of securing because of their high overhead and low dependability. In this work, improved lightweight and dependable trust system for WSNs is proposed. First, a lightweight trust decision-making scheme is proposed based on the nodes' identities (roles) in the clustered WSNs, which is suitable for such WSNs because it facilitates energy-saving. Second direct trust value is calculated using the residual energy calculation and packet transmission between the nodes. Along with the direct trust value calculation, feedbacks cancelling between cluster members (CMs) or between cluster heads (CHs) are also considered. More importantly, considering that CHs take on large amounts of data forwarding and communication tasks, a dependability-enhanced trust evaluating approach is defined for co-operations between CHs. This approach surpasses the limitations of traditional weighting methods for trust factors, in which weights are assigned subjectively. Theory as well as simulation results shows that improved LDTS demands less memory and communication overhead compared with the current typical trust systems for WSNs.

Keywords--- Wireless Sensor Network, Cluster Heads (CH), Cluster Member (CM), Lightweight and Dependable Trust System (LDTS), Base Station (BS)

I. INTRODUCTION

Wireless Sensor Network (WSN) technology is relatively new concept. While wireless communication is already in all sectors of the daily life, WSNs have yet to step beyond the experimental stage. There is a strong interest in the deployment of WSNs in many applications, and the research effort is significant. Due to impressive technological innovations in electronics and communications, small low-cost sensor nodes are available, which can collect and relay environmental data [1]. These nodes have sensing, computing and short range communication abilities and can be deployed in many environments. Such deployment can be in controlled environment such as the sensing of the atmosphere in buildings and factories, where the mobility of the nodes is of interest. Also they can be spread in hazardous and hostile environments and left unattended.

The security issues in WSNs are due to the decentralized nature of the network and absence of infrastructure. In contrast to traditional wireless networks, special security and performance issues have to be carefully considered for sensor networks [2]. For example, due to the unattended nature of sensor networks, an attacker could launch various attacks and even compromise sensor devices

S. Jegadeeshwari, M.Phil, Research Scholar, Dr.N.G.P Arts & Science College, Coimbatore, Tamilnadu, India. E-mail:jegadeeshwarischolar@yahoo.com

R. Balakrishnan, Assistant Professor, Dr.NGP Arts and Science College, Tamilnadu, Coimbatore.

without being detected. Therefore, a sensor network should be robust against attacks, and if an attack succeeds, its impact should be minimized. In other words, compromising a single sensor node or few sensor nodes should not crash the entire network.

Trust in WSN plays an important role in constructing the network and making the addition or deletion of sensor nodes from a network very smooth and transparent. Trust in WSN has been studied lightly by current researchers and is still an open and challenging field. In real-world WSNs, the node cannot be taken as a trustworthy component. Therefore, we have focused on trust model to solve these problems which is beyond the functioning of cryptographic mechanisms. The Sensor node has typically powered batteries; hence it is an additional need to be considered for security purpose. If the authentication mechanism is increased then the energy consumption is more.

However, due to inherent resource and computing constraints, security in sensor networks poses different challenges than traditional network/ computer security. There is currently enormous research potential in the field of wireless sensor network security. Thus, familiarity with the current research in this field will benefit researchers greatly. The main problem in wireless sensor network is Sensor networks are vulnerable to several key types of attacks. Attacks can be performed in a variety of ways, most notably as denial of service attacks, but also through traffic analysis, privacy violation, physical attacks, and so on. In fact, there are a numbers of attacks an attacker can launch against a wireless sensor network once a certain number of sensor nodes have been compromised. In literature, for instance, HELLO flooding attacks, sink hole attacks, Sybil attack [3] , black hole attack , worm hole attacks , or DDoS attacks are options for an attacker. These attacks lead to anomalies in network behaviors that are detectable in general. There are some reported solutions to detect these attacks by monitoring the anomalies.

The main objective of the trust management model proposed in this work is that it should be applied uniformly throughout the sensor network. It should be able to support, through proper configuration, from simple nodes that have very restricted role, computational capabilities and should only trust the nodes they are pre-configured to trust, to highly adaptive nodes and gateways to other networks. In order to overcome high communication overhead and low dependency in existing trust management systems in this research work a novel trust management system for wireless sensor network is proposed. The major objective of the proposed system is to improve the security thus reduces the communication overhead problem in wireless sensor network by using the proposed methodology.

II. RELATED WORKS

Srinjoy et al [4] introduced a novel Trust Integrated Congestion-aware Energy Efficient Routing algorithm (TCEER) in which the potential of a node is computed using its trust value, congestion status, residual energy, distance from the current packet-forwarding node and the distance from the base station using a Fuzzy Logic Controller. The source node selects the node of highest potential in its one hop radio range for data transmission. Hop by hop data routing from source to base station is obtained which is light-weight as well as energy-efficient.

Sultana et al [5] presented a novel lightweight scheme to securely transmit provenance for sensor data. The proposed technique relies on emph{in-packet Bloom filters} to encode provenance. The author introduces efficient mechanisms for provenance verification and reconstruction at the base station. In addition, the author extend the secure provenance scheme with functionality to detect {em packet drop attacks} staged by malicious data forwarding nodes. The author evaluates the proposed technique both analytically and empirically.

Renjian Feng et al [6] introduced a trust management scheme based on revised Dempster-Shafer (D-S) evidence theory. D-S theory is preponderant in tackling both random and subjective uncertainty in the trust mechanism. A trust propagation mechanism including conditional trust transitivity and dynamic recommendation aggregation is developed for obtaining the recommended trust values from third part nodes. The author adopts a flexible synthesis method that uses recommended trust only when no direct trust exists to keep a good trust-energy consumption balance. The author also considers on-off attack and bad mouthing attack in our simulation.

Chen-xu et al [7] propose an improved reliable, trust-based, and energy-efficient data-aggregation protocol for wireless sensor networks. The author called the protocol the iRTEDA protocol, and it combines the reputation system, residual energy, link availability, and a recovery mechanism to improve secure data aggregation and ensure that the network is secure, reliable, and energy-efficient.

Sarma Dhulipala et al [8] introduced a Heuristic Approach based Trust Worthy Architecture for WSN that considers the challenges of the system and focus on the collaborative mechanism for trust evaluation and maintenance. The author presented Architecture could also be capable of fulfilling critical security, reliability, mobility and performance requirements for reliable communication while being readily adaptable to different applications.

Rami et al [9] introduces a Trust model and a Reputation System for wireless sensor nodes in fading multi paths channel. The model establishes the continuous version of the Beta Reputation System applied to binary events. In doing so, the author introduce a theoretically sound Bayesian probabilistic approach for mixing second hand information from neighboring nodes with directly observed information. A Trust model in a wireless sensor network addresses the security issue and how to deal with possibly malicious and unreliable nodes. Although encryption and cryptography keys are used, these deterministic approaches fail to answer the problem of securing the routing and content of information through a network. Reputation systems are developed to combine with deterministic measures to secure the integrity of a network.

Tanveer & Albert [10] presented a computationally lightweight security framework to provide a comprehensive security solution against the known attacks in sensor networks. This framework consists of four interacting components: a secure triple-key scheme (STKS), secure routing algorithms (SRAs), a secure localization technique (SLT) and a malicious node detection mechanism. Singly, each of these components can achieve certain level of security. However, when deployed as a framework, a high degree of security is achievable. The framework takes into consideration the communication and computation limitations of sensor networks. While there is always a tradeoff between security and performance, experimental results prove that the proposed framework can achieve high degree of security with negligible overheads.

William & Dongwan [11] introduced an approach to protecting wireless sensor networks based on a security policy, enforced at the node level. This policy is based on a new approach to key establishment, which combines a group-based distribution model and identity-based cryptography. Using this solution enables nodes to authenticate each other, and provides them with a structure to build secure communications between one another, and between various groups. Using key establishment protocol and security policy, the author shows how to reduce or prevent significant attacks on wireless sensor networks.

Vinod et al [12] derived a new representation for the collusive sensor nodes when the underlying fraudulent correlated environment has strong influence on wireless sensor networks performance. The author had evaluated collusion effect with respect to static (SW) and dynamic (DW) wireless sensor networks to derive the joint resultant. Moreover accuracy, path length, and energy consumption of sensor node operations are also evaluated. Additionally, the author emphasized over the satisfaction evaluation for linguistic fuzzy trust and reputation (LFTM) models in the deployed WSN framework.

III. Proposed Methodology

A. *Network Topology Model and Assumptions*

Our primary goal is to develop a trust-based framework for cluster-based WSNs as well as a mechanism that reduces the likelihood of compromised or malicious nodes being selected (or elected) as collaborative nodes. A node in the clustered WSN model can be identified as a CH, or a CM. Members of a cluster can communicate with their CH directly. A CH can forward the aggregated data to the central BS through other CHs. In this research work the aim assumption to calculate the trust are the nodes are organized into clusters with the help of a proposed clustering scheme such as Heinzelman et al [13] and also all nodes have unique identities, which is similar to the assumptions. In a number of sensor network models, nodes do not have unique identities similar to the Internet protocol in traditional networks. However, to uniquely identify nodes and to perform communication in such environments, a class-based addressing scheme is used, in which a node is identified by a triplet.

$$< \text{location, node type, node subtype} >$$

To protect trust values from traffic analysis or fabrication during transfer from one node to another, a secure communication channel is assumed, and it can be established by using any key management scheme.

B. *Improved Lightweight Scheme for Trust Decision-Making*

Improved LDTS needs to maintain two levels of trust: intercluster trust and intracluster trust. Intracluster trust evaluation has two kinds of trust relationship: CM-to-CM direct trust and CH-to-CM feedback trust. Likewise, intercluster trust evaluation also has two kinds of trust relationship, CH-to-CH direct trust and BS-to-CH feedback trust.

Proposed CM-to-CM Direct Trust Calculation

The trust evaluation approach at CMs is defined by the following equation:

$$P_{x,y} = \left[\left(\frac{10 \times s_{x,y}(\Delta t)}{s_{x,y}(\Delta t) + u_{x,y}(\Delta t)}\right)\left(\frac{1}{\sqrt{u_{x,y}(\Delta t)}}\right)\right] \qquad (1)$$

$s_{x,y}(\Delta t)$ is the total number of successful interactions of node x with y during past time Δt. $u_{x,y}(\Delta t)$ is the total number of unsuccessful interactions of node x with y during past time Δt. The expression $\frac{1}{\sqrt{u_{x,y}(\Delta t)}}$ denotes approaches 0 rapidly with an increase in the number of unsuccessful interactions, which indicates the strict punishment feature of LDTS for unsuccessful interactions.

$N_{x,y}^{energy}$ refers to the belief of node x that node y still has adequate energy (representing competence) to perform its intended function. The energy may be measured for each and every sensor node by using the formula

$$N_{x,y}^{energy} = N_{x,y}^{intial\ energy} - N_{x,y}^{consumedenergy} \qquad (2)$$

Consumed Energy Calculation

$$N_{x,y}^{consumedenergy} = k\left\{\sum_{i=1}^{n}\left[2 * e_{elec} + e_{amp}\,(d_i)^{\alpha}\right]\right\} \qquad (3)$$

Where e_{elec} represents energy consumed intransmission, e_{amp} amplification, k the message length, d the transmitter/receiver distance and α a factor describing attenuation. Therefore to trust value is calculated as

$$T_{ij}^{X}(t) = (1-\alpha)N_{x,y}^{energy} + \alpha P_{x,y} \qquad (4)$$

A CM calculates the trust value of its neighbors based information available by observing directly. Trust value is evaluated by packet transmission and energy calculation of each node using the formula mentioned above. One of the important constraints to calculate trust value in proposed work is neighborhood nodes feedback from CH. All CMs communicate via a shared bidirectional wireless channel and operate in the promiscuous mode; the source node should first get the feedback from the cluster head. Then source node analysis the packet transmission history of that node along with remaining energy of the node. The trust value is calculated using the remaining energy value and packet transmission history. If does not overhear the retransmission of the packet within a threshold time from its neighboring node or if the overheard packet is found to be illegally fabricated (by comparing the payload that is attached to the packet), then will it is considered as not trust value).

CH-to-CM Feedback Trust Calculation

Supposing the existence of $(n-1)$ CMs in a cluster. The cluster head Ch will periodically broadcast the request packet within the cluster. In response, all CMs in the cluster will forward their trust values toward other CMs to Ch. Then, Ch will maintain these trust values in a matrix, as shown below:

$$H = \begin{pmatrix} T_{1,1} & T_{1,2} & \cdots & T_{1,n-1} \\ T_{2,1} & T_{2,2} & \ddots & T_{2,n-1} \\ T_{n-1,1} & T_{n-1,2} & \cdots & T_{n-1,n-1} \end{pmatrix} \tag{5}$$

Where $T_{x,y}(x \in [1, n-1], y \in [1, n-1])$ is the direct trust of node on . On the other hand, which means this value is a node's ratings towards itself. To reduce boasting, this value will be discarded by during feedback trust aggregation. Whitby et al [14] presented the beta feedback system, which is based on the theory of statistics and is characterized by flexibility and simplicity. The beta probability density functions is used to compute $R_{ch,y}(\Delta t)$

$$R_{ch,y}(\Delta t) = \lceil 10 \times E(\varphi(p|r,v)) \rceil \tag{6}$$

where $\lceil\cdot\rceil$is the nearest integer function, p denotes the posteriori probabilities of binary events (r, v) , r is the amount of positive feedback towards $(T_{x,y} \geq 5)$ node counted from matrix , and is the amount of negative feedback $(T_{x,y} \geq 5)$ towards node y. $E(\varphi(p|r,v))$ is the probability expectation value of the beta distribution $\varphi(p|r,v)$

$$E(\varphi(p|r,v)) = \frac{r+1}{r+v+2} \tag{7}$$

Analyzing feedback aggregation mechanism is found to be a lightweight method with very simple mathematical formulas, which is suitable for resource-constrained nodes in a large-scale sensor network. However, a possible attack scenario to the trust system must be considered.

If a CH behaves badly in indirect trust feedback to its CMs, the CMs will have no idea that the feedback from the CH is actually misleading. Thus, the selection of a trustworthy node as the CH is one of the most significant requirements in cluster WSNs. This problem has been studied by several scholars. In TCHEM Crosby et al [15], Crosby et al. proposed a novel selection mechanism to reduce the likelihood of a malicious node to be selected as a CH. In Ferdous et al [16] presented an interesting scheme for the selection of a trustworthy CH that can provide secure communication via cooperative nodes. To make ILDTS independent of any specific clustering protocol, in this work, a trustworthy node has been selected as the CH of the cluster by using any selection protocol. That is, assumed that CH is trustworthy within its cluster.

Dependability-Enhanced Intercluster Trust Evaluation

In accordance with the characteristics of clustered WSNs, both CMs and CHs are resource-constrained nodes, and BSs have more computing and storage capacity and no resource constraint problem. Thus, energy conservation remains a basic requirement for trust calculation at CHs.

CH-to-CH Direct Trust Calculation: During CH-to-CH communication, the CH maintains a record of past interactions with other CHs in the same manner as CMs keep records of other CMs. The direct trust between a CH toward another CH is defined as:

$$P_{i,j}(\Delta t) = \left\lceil \left(\frac{10 \times S_{i,j}(\Delta t)}{S_{i,j}(\Delta t) + U_{i,j}(\Delta t)} \right) \left(\frac{1}{\sqrt{U_{i,j}(\Delta t)}} \right) \right\rceil \tag{8}$$

where $U_{i,j}(\Delta t) \neq 0. S_{i,j}(\Delta t)$ is the total number of successful interactions of CH i with CH j during time window Δt , and $U_{i,j}(\Delta t)$ is the total number of unsuccessful interactions of CH i with CH j . As a special case, if $S_{i,j}(\Delta t) \neq 0$ and $U_{i,j}(\Delta t) = 0$, set $C_{i,j}(\Delta t) = 10$.

E_c^{energy} refers to the belief of node x that node y still has adequate energy (representing competence) to perform its intended functions. The energy may be measured for each and every sensor node by using the formula

$$E_c^{energy} = E_c^{intial\ energy} - E_c^{consumedenergy} \tag{9}$$

Consumed Energy Calculation

$$E_c^{consumedenergy} = k\left\{\sum_{i=1}^{n}\left[2 * e_{elec} + e_{amp}\,(d_i)^{\alpha}\right]\right\} \tag{10}$$

Where e_{elec} represents energy consumed intransmission, e_{amp} amplification, k the message length, d the transmitter/receiver distance and α a factor describing attenuation.

Therefore to trust value is calculated as

$$C_{ij}^{X}(t) = (1-\alpha)E_c^{energy} + \alpha P_c \tag{11}$$

BS-to-CH Feedback Trust Calculation: Supposing that CHs exist in the network. The base station bs will periodically broadcast the request packet within the network. In response, all CHs in the network will forward their direct trusts for other CHs to bs. bs will maintain these trust values in a matrix , as shown below:

$$B = \begin{pmatrix} C_{1,1} & C_{1,2} & \cdots & C_{1,m} \\ C_{2,1} & C_{2,2} & \ddots & C_{2,m} \\ C_{m,1} & C_{m,2} & \cdots & C_{m,m} \end{pmatrix} \tag{12}$$

where is the direct trust of CH toward CH . Moreover, i = j, which means that this value is a CH's ratings for itself. To reduce boasting, this value will be discarded by the BS during feedback trust aggregation. One of the difficulties of computing for BS-to-CH feedback trust is the question of malicious feedback. Liang & Shi [17] found that the lightweight average aggregation algorithm performs better than complex algorithms, especially when a considerable number of bad raters exist in the system. An enhanced beta probability density function to compute for BS-to-CH feedback trust:

$$F_{bs,j}(\Delta t) = \left\lceil \frac{10 \times E\big(\varphi(p|g,l)\big) + \overline{C_{k,j}}(\Delta t)}{2} \right\rceil \tag{13}$$

Where p denotes the posteriori probabilities of binary events (g,l), g is the amount of positive feedback $\left(C_{k,j} \geq 5\right)$ towards a CH j, and l is the amount of negative feedback $\left(C_{k,j} \geq 5\right)$.

$$E\big(\varphi(p|g,l)\big) = \frac{g+1}{g+l+2} \tag{14}$$

which is the probability expectation value of the beta distribution function $\varphi(p|g,l)$. $\overline{C_{k,j}}$ is the average value of aggregated feedback from $(g+1)$ CHs in the network:

$$\overline{C_{k,j}}(\Delta t) = \frac{\sum_{k=1}^{g+l} C_{k,j}(\Delta t)}{g+l} \tag{15}$$

Where $C_{k,j}(\Delta t)$ is the feedback of CH k toward CH j. Analyzing the aforementioned equations BS-to-CH feedback mechanism not only considers the amount of feedback $(g+1)$, but also considers the quality of each feedback$\left(C_{k,j}(\Delta t)\right)$. Therefore, approach is more aligned with the habit of human cognition on feedback, which is an innovation of LDTS beyond approaches Boukerche et al [18].

Self-Adaptive Global Trust Aggregation at CHs: the GTD of a CH comprises two parts (which is adopted by most studies on trust management): the firsthand trust (CH-to-CH direct trust) and the secondhand trust (BS-to-CH feedback trust). Thus, the CH 's GTD is aggregated by the following equation:

$$O_{i,j}(\Delta t) = \left\lceil 10 \times \left(w_1 \times C_{i,j}(\Delta t) + w_2 \times F_{i,j}(\Delta t)\right)\right\rceil \tag{16}$$

Where $\lceil\cdot\rceil$ is the nearest integer function. w_1 is the weight of $C_{i,j}(\Delta t)$, and correspondingly, w_2 is the weight of $F_{i,j}(\Delta t)$. The weights w_1 and w_2 meet $w_1 + w_2 = 1$. $C_{i,j}(\Delta t)$ and $F_{i,j}(\Delta t)$ can be computed according respectively. However, the level of accuracy of the values of w_1 and w_2 is a key question to be considered by this work.

How to avoid the effect of individual favoritism on the weight allocation of trust sources is a key task of trust management. In this work, a self-adaptive approach to calculate is defined the values of w_1 and w_2 :

$$w_1 = \frac{\Phi(S)}{\Phi(S)+\Phi(g)}, w_2 = \frac{\Phi(g)}{\Phi(g)+\Phi(S)}$$

Where $\Phi(S) \in [0,1]$ and S denote the total amount of successful interactions of CH $i$with j during Δt . $\Phi(g) \in [0,1]$is called the feedback factor. Constant g is provided by the BS, g is the amount of positive feedback $\left(C_{k,j} \geq 5\right)$

toward CH . $\Phi(x)$ is a positive function that increases with the number of positive feedback g or the total amount of successful interactions , which is defined as follows:

$$\Phi(x) = 1 - \frac{1}{\alpha + x}$$

Where $\alpha \geq 0$ is a positive constant that can be tuned by the trust system accordingly. The function $\Phi(x)$ has a desirable property in that with increasing α (α could be any positive integer), the function quickly approaches 1. The choice of the above function is aimed at brevity and ease of calculation. The feedback factor $\Phi(g)$ is found to approach 1 rapidly with increasing α and positive feedback g. To increase the dependability of the trust system, suggest that a smaller value of, such as $\alpha = 1$, be set. Thus, the value of $\Phi(g)$ primarily depends on the amount of positive feedback. For example, if $\alpha = 1, g = 4$ then $\Phi(g) = 1 - 1/(1+4) = 0.80$.

IV. Experimental Results

In order to validate the proposed model and the algorithms and metrics that it includes implementation of a simulation environment in ASP.net. In this section, the simulation setup is described and parameterization, the network model and the node configuration of the simulation scenario. In this research work, the three parameters are considered here they are communication overhead, throughput and PSDR ratio. The results that were obtained in terms of the established trust relationships are discussed in this section along with the required operations, their distribution among the network nodes, and the results of the trust revocation operations.

In the simulator, three kinds of nodes exist 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.

Improved LDTS works with two topologies: the intercluster (CH-to-CH) topology, where distributed trust management is used, and intracluster (CM-to-CM) topology, where the centralized trust management approach is employed. The different calculation mechanisms are employed for intracluster and intercluster trust evaluations. According to these characteristics of LDTS, in this simulator, the performance of ILDTS is evaluated based on intracluster and intercluster cases. This approach will not affect the results of performance evaluation and will greatly reduce the complexity of the simulator. The simulation parameters and default values used in the experiments are listed in Table 5.1.

Table 5.1: Simulation Parameters and its Values

Symbol	Description	Possible values
$N = m \times n$	The number of nodes	160-1800
n	The number of CMs in a cluster	8-18
m	The number of clusters	20-100
t	Time steps of simulation runs	1000

Communication Overhead Analysis and Comparison

To evaluate the communication overhead under full-load conditions, assume a worst-case scenario, in which every CM wants to communicate with every other CM in the cluster, and every CH wants to communicate with the rest of the CHs in the network. At the same time, each CH needs to collect feedback reports from its CMs, and the BS has to collect feedback reports from its CHs. Let us assume that the network consists of m clusters and that the average size of clusters is (including the CH of the cluster).

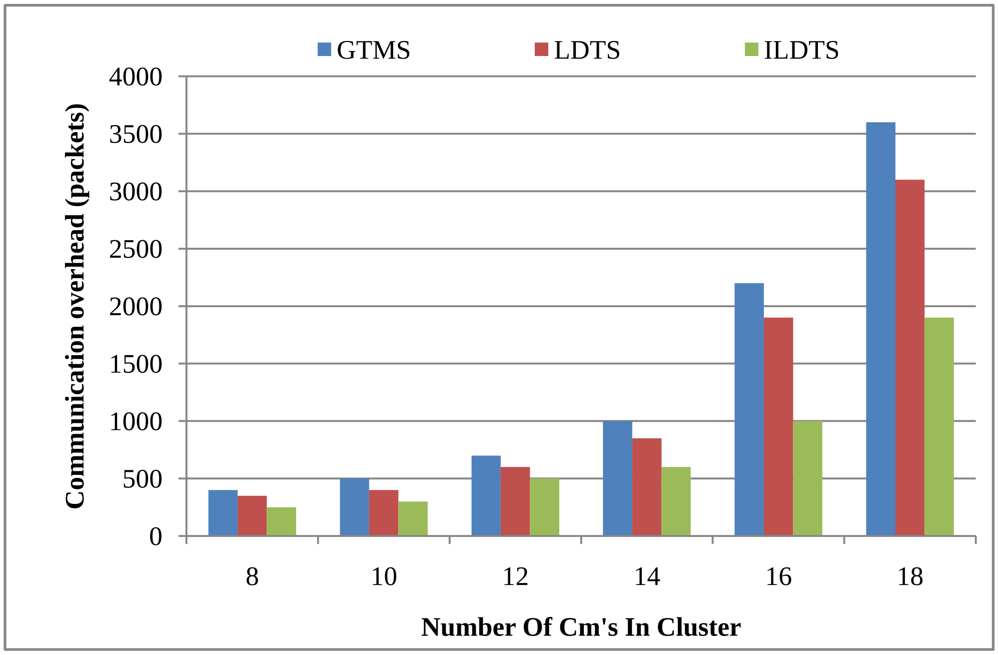

Fig. 1: CM-to-CM Communication Overhead in a Cluster

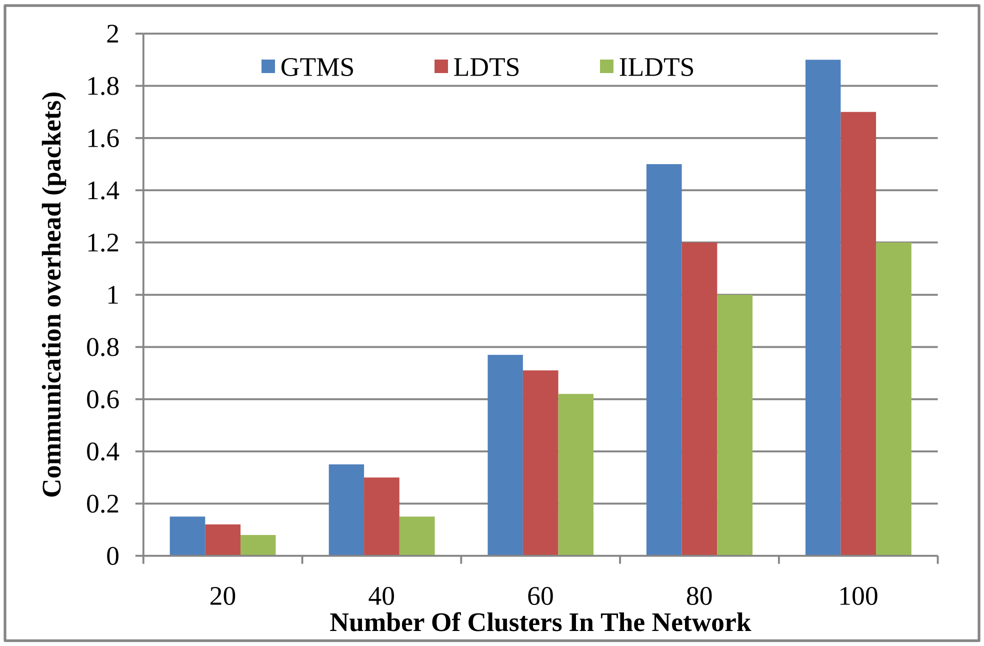

Fig. 2: CH-to-CH Communications Overhead in a Network

Fig 1 and 2 shows the comparison results of the CH-to-CH communication overhead between LDTS and GTMS. LDTS and GTMS have a relatively close network overhead as the network size increases, which indicates that both LDTS and GTMS are suitable for large-scale clustered WSNs.

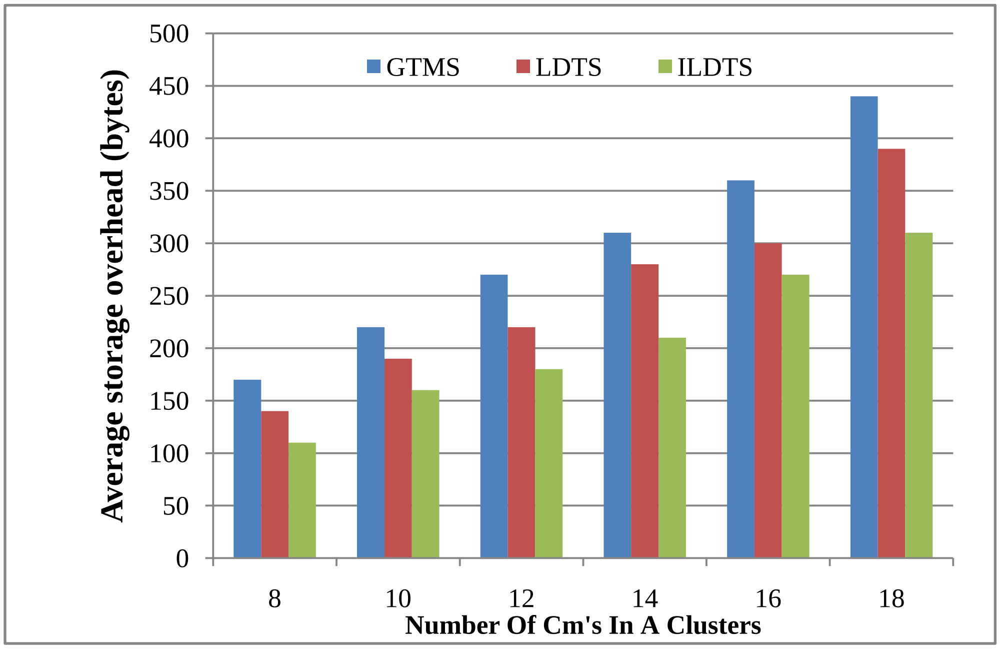

Fig. 3P: Average Storage Overhead at Each CM in a Cluster

Fig 3 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.

Packet Successful Delivery Ratio (PSDR)

PSDR is to reflect the dependability of trust management systems. A higher PSDR indicates higher dependability. Assume that most of CMs and CHs are good in the WSN community, where BCMs and BCHs each comprise only 10%. This WSN environment closely resembles a real situation, where most CMs are honest and most CHs are good.

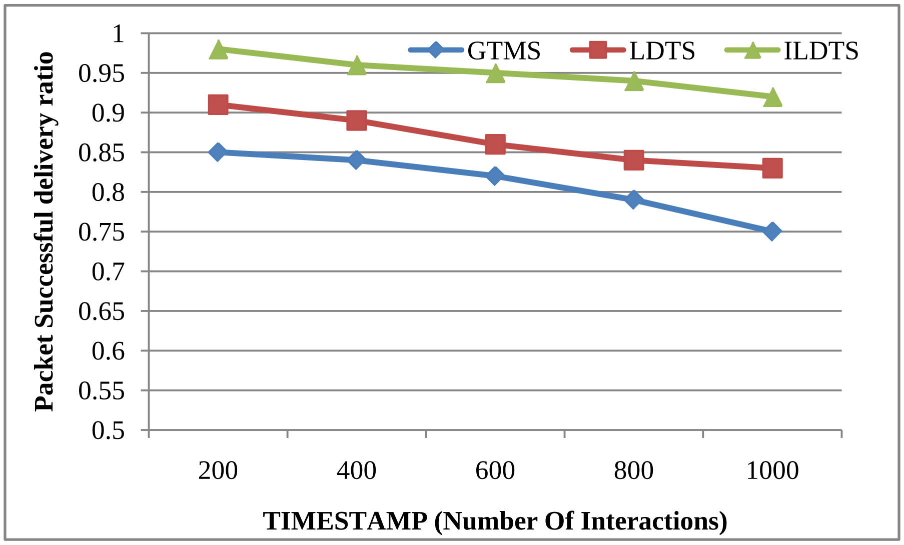

Fig. 4: PSDR Comparison with Different Percentages of MCHs. (a) MCH 5%.

Fig 4 shows the PSDR comparison results under different percentages of malicious cluster heads (MCHs). In this group simulation, considered WSN community, where 95% of CMs are honest. The remaining 5% of CMs are MCMs. the percentage of MCHs as 5%, 10%, and 20% are fixed separately which respectively indicate that the WSN environment is honest, relatively honest, and dishonest community, with 50, 100, and 200 dishonest CHs separately. Fig 5 shows an honest WSN environment, where the percentage of MCHs is only 5%. The proposed algorithm improved LDTS have a high PSDR, which reflects that have a high dependability under an honest WSN environment. These results are consistent with a real situation, i.e., in a dishonest WSN community, malicious CHs may conduct a bad-mouthing attack, which can greatly affect the performance of the WSN system. This can significantly improve the dependability of ILDTS.

Throughput

It is the number of packets successfully received by the receiver.

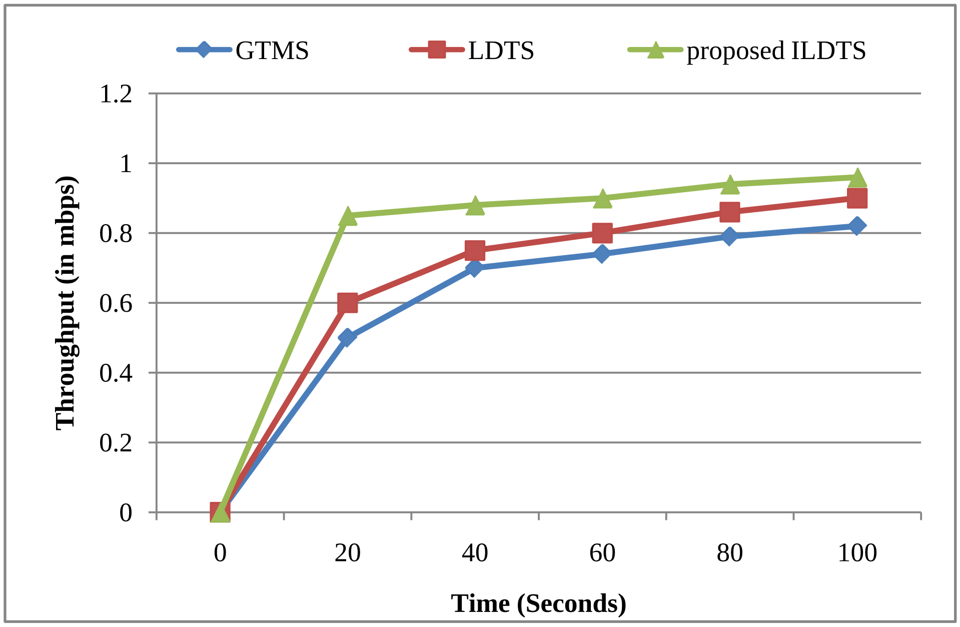

Fig. 5: Comparison of throughput for Different Trust Based Systems

The graphical representation of throughput comparison is shown in the Fig.5. The graph shows that the proposed protocol is better than the existing protocols such as GTMS and LDTS.

V. Conclusion

In this work, improved LDTS for clustered WSNs is proposed. The proposed system reduces malicious nodes using the proposed direct trust value calculation for each and every node in the network. The direct trust value calculation is based on the energy efficiency and packet transmission between the nodes. By adopting a dependability-enhanced trust evaluating approach for co-operations between CHs, improved LDTS can effectively detect and prevent malicious, selfish, and faulty CHs. The parameters used for performance evaluation of the proposed system are communication overhead, throughput analysis and packet successful delivery ration (PSDR). The proposed system greatly reduces the communication overhead compared to the existing system. With the increasing the number of Cluster's the CM-to-CM and CH to CM communication overhead of ILDTS slowly increased with the increasing number of Clusters. Future research work in trust management focuses on generalized, scalable and reconfigurable trust model suitable for distributed computing system. It handles malicious and non malicious misbehavior in networking, sensing and data processing.

This can improve the security issues to meet specific application demands.

REFERENCE

[1]. "Wireless sensor networks: a survey", I.F Akyildiz, W. Su, Y. Sankara subramaniam and E. Cayirci. Computer Networks 2002: 38(4): 393-422.

[2]. "A Hybrid Trust Based Secure Model For Wireless Sensor Network", S Mohan Kumar, R Thenmozhi, A Inian Lourde Alex and M Malarvizhi, , International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 3, Issue 1, pp.144-147, January – February 2014

[3]. "Malicious Node Detection in Wireless Sensor Networks using Weighted Trust Evaluation", Idris M. Atakli, Hongbing Hu, Yu Chen, Wei-Shinn Ku and Zhou Su , Proceedings of the 2008 Spring simulation multiconference, Pages 836-843,2008.

[4]. "A Trust-based Framework for Congestion-aware Energy Efficient Routing in Wireless Multimedia Sensor Networks" , Srinjoy Ganguly, Arpita Chakraborty and Mrinal Kanti Naskar, Networking and Internet Architecture (cs.NI), arXiv:1312.4071 [cs.NI],2013.

[5]. "A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks in Wireless Sensor Networks", S. Sultana, ; G. Ghinita,. ; E. Bertino and M Shehab, IEEE Transactions on Dependable and Secure Computing, Volume:PP , no: 99, 2013.

[6]. "Trust Management Scheme Based on D-S Evidence Theory for Wireless Sensor Networks", Renjian Feng, Shenyun Che, Xiao Wang, and Ning Yu, International Journal of Distributed Sensor Networks Volume 2013 (2013), Article ID 948641, 9 pages.

[7]. "Improved Reliable Trust-Based and Energy-Efficient Data Aggregation for Wireless Sensor Networks", Chen-xu Liu, Yun Liu, and Zhen-jiang Zhang, International Journal of Distributed Sensor Networks Volume 2013 (2013), Article ID 652495, 11 pages.

[8]. "A Novel Heuristic Approach Based Trust Worthy Architecture for Wireless Sensor Networks", V. R. Sarma Dhulipala, N. Karthik and RM. Chandrasekaran, Wireless Personal Communications , Volume 70, Issue 1, pp 189-205 , May 2013

[9]. "Trust and Reputation Analysis in Fading Wireless Sensor Network Channel", Rami Al-Hmouz , Mohammed Momani and Maen Takruri , Life Science Journal 2013;10(4),pp.310-318.

[10]. "A Lightweight Security Framework for Wireless Sensor Networks", Tanveer A. Zia and Albert Y. Zomaya Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 2, number: 3, pp. 53-73,2011.

[11]. "A novel node level security policy framework for wireless sensor networks", William R. Claycomb and Dongwan Shin, Journal of Network and Computer Applications, Volume 34, Issue 1, Pages 418–428, January 2011.

[12]. "Collusion Based Realization of Trust and Reputation Models in Extreme Fraudulent Environment over Static and Dynamic Wireless Sensor Networks", Vinod Kumar Verma,Surinder Singh, and N. P. Pathak, International Journal of Distributed Sensor Networks Volume 2014 (2014), Article ID 672968, 9 pages

[13]. "Filtering out unfair ratings in bayesian reputation systems,", A. Whitby, A. Jøang, and J. Indulska, The Autonomous Agents and Multi Agent Systems 2004, New York, Jul. 2004.

[14]. "An application-specific protocol architecture for wireless microsensor networks,", W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan , IEEE Trans. Wireless Commun., vol. 1, no. 4, pp. 660–670,Oct. 2002.

[15]. "A framework for trust-based cluster head election in wireless sensor networks,", G. V. Crosby, N. Pissinou, and J. Gadze, in Proc. Second IEEEWorkshop on Dependability and Security in Sensor Networks and Systems, 2006, pp. 10–22.

[16]. "Trust-based cluster head selection algorithm for mobile ad hoc networks," R. Ferdous, V. Muthukkumarasamy, and E. Sithirasenan, in Proc. 2011 Int. Joint Conf. IEEE TrustCom-1111/IEEE ICESS-11/FCST-11, pp. 589–596.

[17]. "TRECON: A trust-based economic framework for efficient internet routing," Z. Liang and W. Shi, IEEE Trans. Syst., Man, Cybern. A, Syst., Humans, vol. 40, no. 1, pp. 52–67, Jan. 2010.

[18]. "Trust-based security for wireless ad hoc and sensor networks," A. Boukerche, X. Li, and K. EL-Khatib, Computer Commun., vol. 30, pp. 2413–2427, Sep. 2007.