ijecs open access www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 6 June, 2014 Page No. 6706-6712

Trust Decision Making Scheme for Wireless Sensor Networks

Veena A[1], Kavyashree S C[2]

[1]Department of Computer Science and Engineering
Channabasaveshwara Institute of Technology
Gubbi, Karnataka, India.
veena.a@cittumkur.org

[2]Department of Computer Science and Engineering
Channabasaveshwara Institute of Technology
Gubbi, Tumkur Dist, Karnataka, India
kavyashree1689@gmail.com

Abstract: ***The fundamental requirements for any wireless sensor network (WSN) are network life time, resource efficiency and dependability of a trust system. We are applying a clustering scheme considering mobility to minimize the number of nodes that moves away from the current cluster head before next cluster formation. This approach improves network life time and energy consumption. In addition, we use trust decision-making scheme based on the node's identities in the clustered MWSNs to send data packets to sink. It facilitates energy-saving by canceling feedback between cluster members (CMs) or between cluster heads (CHs), which is suitable for WSNs. This approach can significantly improve system efficiency, while reducing the effect of malicious nodes, selfish, and faulty CHs of networking consumption. Theory as well as simulation results show that clustering scheme improves network lifetime and dependable trust decision making scheme demands less memory and communication overhead compared with the current typical trust systems for WSNs.***

Keywords— clustering; self-adaptivity; trust management; trust model; wireless sensor network; data aggregation.

I. INTRODUCTION

In present day wireless sensor network (WSN) has become one of the most interesting networking technologies since it can be deployed without communication infrastructures. A sensor network is composed of a large number of sensor nodes and a sink. The base station (BS) of WSN typically serves as a gateway to some other networks which provides a powerful data processing, storage center, and an access point to the sensor nodes in its network. Sensor nodes sense their environment, collect sensed data and transmit it to the BS but their power, computational capacity and memory are limited due to non grouping among the nodes. For cluster wireless sensor networks (WSNs) such as Low-Energy Adaptive Clustering Hierarchy (LEACH), EEHC, EC, and HEED, network scalability and throughput can be effectively improved by adopting clustering algorithms by which nodes are grouped into clusters, and within each cluster a node with strong computing power is elected as a cluster head (CH). CHs together form a higher-level backbone network and after several recursive iterations, a clustering algorithm constructs a multilevel WSN structure, this structure facilitates communication and enables the restriction of bandwidth-consuming network operations such as flooding only to the intended clusters. Establishing trust in a clustered environment provides numerous advantages, such as enabling a CH to detect faulty or malicious nodes within a cluster. In the case of multi loop clustering, a trust system aids in the selection of trusted routing nodes through which a cluster member (CM) can send data to the CH. During inter cluster communication, a trust system also aids in the selection of trusted routing gateway nodes or other trusted CHs through which the sender node will forward data to the base station (BS). A number of studies have proposed the work on WSNs.

However, these systems suffer from various limitations such as the incapability to meet the resource constraint requirements of the WSNs, more specifically, for the large-scale WSNs. Recently, very few trust management systems have been proposed for clustered WSNs, such as GTMS, TCHEM, HTMP, and ATRM. To our best knowledge, a universal trust system designed for clustered WSNs to achieve dependability and resource efficiency remains lacking. G. S. Kumar proposed LEACH which was the very first protocol that uses clustering to increase the life time of WSNs. In LEACH, cluster heads are randomly selected by turns with a certain probability in order not to drain the battery of a single sensor node this improves the performance in terms of evenly energy dissipation, but its applications are limited to fixed sensor nodes only due to non consideration of mobility of the sensor nodes after the setup phase for cluster head selection within a round this losses a serious of data in MWSNs. GTMS for clustered WSNs which evaluates the trust of a group of nodes in contrast to traditional trust schemes that always focus on the trust values of individual nodes was developed by sheik et.al, which gives WSNs the benefit of requiring less memory to store trust records at each node. GTMS aids in the significant reduction of

the cost associated with the trust evaluation of distant nodes but GTMS relies on a broadcast-based strategy to collect feedback from the CMs of a cluster, which requires a significant amount of resources and power.

Bao *et al.* proposed HTMP, for cluster-based WSNs that consider two aspects of trustworthiness: social trust and QoS (quality-of service) trust. Probability model utilizing stochastic Petri net techniques to analyze protocol performance and then validated subjective trust against the objective trust was developed based on ground truth node status. However, implementing such a complex trust evaluation scheme at each CM of the cluster is unrealistic.

Crosby *et al.* proposed TCHEM, a trust-based cluster head election mechanism. Its framework is design in the context of a cluster-based network model with nodes that have unique local IDs. This approach can decrease the likelihood of malicious or compromised nodes from becoming CHs. The mechanism does not encourage sharing of trust information among sensor nodes. Thus, this approach reduces the effect of bad mouthing attacks. However, TCHEM does not cover trust in detail, because of which numerous key issues of trust management are not introduced.

Boukerche *et al.*proposed ATRM, an agent-based trust and reputation management scheme. ATRM introduces a trust and reputation local management strategy with the aid of the mobile agents running on each node. The benefit of a local management scheme for trust and reputation is that centralized repositories are not required, and the nodes themselves capable of providing their own reputation information whenever requested. Therefore, reputation computation and propagation is performed without network-wide flooding and with no acquisition- latency. However, ATRM assumes that mobile agents are resilient against malicious nodes that try to steal or modify information that such agents carry. In numerous applications, this assumption may be unrealistic.

By considering all the disadvantages in the trust management systems on WSNs we proposed and used both clustering scheme and trust management system for WSNs in which all nodes calculate their waiting time using the potential score which selects a cluster head candidate and rest of the nodes other than the cluster heads join the best effective cluster head based on the link connection time (LCT) and energy consumption parameters. This approach reduces the number of nodes leaving the cluster and also overcomes the limitations of traditional weighting methods for trust factors, in which weights are assigned subjectively as a result the network life time and resource efficiency have been increased.

II. Clustering Scheme

1.1 Cluster Head Selection

Cluster Head is selected using potential score and link connection time .Each node calculates potential score and link connection time. Node with highest potential score and link connection time is selected as a cluster head.

Potential Score: It is calculated considering three factors mobility, residual energy and density [8].

$$PS=w_{1*}\,SM+\,w_{2*}DE+\,w_{3*}DD \qquad (1)$$

Where w1, w2 and w3 are weighting factors that can be selected based on application.

Similarity of Movement: Similarity of movement is a correlation related to the similarity of speed and direction of movement with its neighbors. The node with lowest SM moves at close to the mean speed and movement direction of their neighbors.

Degree of Residual Energy (DE): The residual energy is a remaining energy in a node after the transmission of a packet. The residual energy has been drastically reduced for each transmission.

This residual energy is a critical resource in WSN. Degree of Residual energy is calculated using

$$DE = (1-E_{Res}/E_{Ini}) \qquad (2)$$

Where E_{Res} is the residual energy and $_{EIni}$ is the initial energy of node.

Degree of Density (DD): The density of each node can be calculated as follows:

$$DD = (\,1-D_{Ni}\,/D_{Avg}\,) \qquad (3)$$

Where D_{Ni} is the number of nodes in the cluster and D_{Avg} density of all nodes.

Link Connection Time: It is defined as amount of time neighboring nodes stay connected. During the LCT, two mobile nodes will remain connected within the transmission range of each other. To organize a stable cluster, node with longest LCT with its neighbors is selected as cluster head.

Let (*xi*,*yi*) be the coordinated of cluster head and (*xj*,*yj*) be that of mobile sensor node *N*. Also the cluster head and mobile sensor node *N* move to the moving angel θi and θj with speed *vi* and *vj*, respectively.

LCT can be predicted using the mobility of node such as the speed and moving direction as below Eq(4). [11-12].

$$LCT = \frac{-(ab+cd)+\sqrt{(a^2+c^2)r^2-(ad-bc)^2}}{a^2+c^2} \qquad (4)$$

where $a=vicos\theta i-vjcos\theta j$, $b=xi-xj$, $c=visin\theta i-vjsin\theta j$ and $d=yi-yj$. If two nodes have zero relative velocity, *i.e.*, $vi=vj$ and $\theta i=\theta j$, the link will remain forever as *LCT* will be ∞.

Algorithm for Cluster Head Selection

1. All nodes calculate Similarity of movement(SM), Degree of Energy(DE) and Degree of Density(DD)
2. Each node calculate Link Connection Time (LCT)
3. All nodes calculate Potential Score (PS) which is a sum of Similarity of movement(SM), Degree of Energy (DE) and Degree of Density (DD)
4. All nodes exchange potential score and link connection time values
5. Node with highest potential score and link connection time value is elected as a cluster head.
6. The cluster head broadcasts elected information to all other nodes.

1.2 Data Aggregation Operation

After Cluster is organized, when event occurred nearer nodes collects the surrounding information. Cluster head determines the number of members through request and acknowledgement. During the request period cluster

head broadcasts its location, velocity and the amount of energy. Each node received the request sends an acknowledgement to its cluster head. Cluster head creates a TDMA schedule and sends to its members. All member nodes send collected data at assigned slot to its cluster head.

Algorithm for Data Aggregation

1. Cluster Head sends request to cluster members along with its location, velocity and the amount of energy.
2. The nodes which receive the request send acknowledgement to the Cluster Head.
3. Cluster Head creates TDMA schedule and sends to its members.
4. Members send the collected data to Cluster Head at assigned time slot.
5. Cluster Head aggregates data sent by its member nodes.

The proposed system can prolong network lifetime nodes consume less energy for receiving and transmitting the data because the distance between cluster head and members are small due to the consideration of density. If cluster head and member move with similar mobility, it can reduce the cost for node to join a new cluster head. In addition, node with longest link connection with its neighbours is elected as a cluster head so it reduces the frequent disconnection between cluster head and its members. We have used a TDMA approach which avoids intra-cluster collisions.

The proposed system can prolong network lifetime nodes consume less energy for receiving and transmitting the data because the distance between cluster head and members are small due to the consideration of density. If cluster head and member move with similar mobility, it can reduce the cost for node to join a new cluster head. In addition, node with longest link connection with its neighbors is elected as a cluster head so it reduces the frequent disconnection between cluster head and its members. We have used a TDMA approach which avoids intra-cluster collisions.

III. TRUST DECISION-MAKING SCHEME

3.1 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 (See Fig. 1). 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 traditional networks a number of sensor network models, nodes do not have unique identities similar to the Internet protocol. 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 <location, node type, node subtype>. We also assume a secure communication channel to protect trust values from traffic analysis during transfer from one node to another.

3.2 Core Design Issues of Trust Establishment Methods

Trust can be established in a centralized or distributed manner. Obviously and sensor networks prefer distributed trust management, where each network entity maintains a trust manager.

The basic elements of such a trust manager are illustrated in Fig. 2 and described in this section.

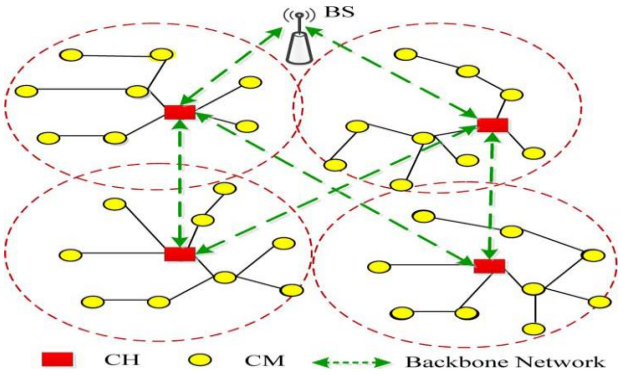

Figure 1: Roles and identities of nodes in a clustered WSN model

The trust record stores information about trust relationships and associated trust values. A *trust relationship* is always established between two parties for a specific action. That is, one party trusts the other party to perform an action. In this work the first party is referred to as the *subject* and the second party as the *agent*. A notation: {*subject*: *agent*, *action*} is introduced to represent a trust relationship. For each trust relationship, one or multiple numerical values, referred to as *trust values*, describe the level of trustworthiness.

There are two common ways to establish trust in computer networks is first, when the subject can directly observe the agent's behavior, *direct trust* can be established and second, when the subject receives recommendations from other entities about the agent, *indirect trust* can be established.

Direct trust is established through observations on whether the previous interactions between the subject and the agent are successful. The observation is often described by two variables: *s*, denoting the number of successful interactions, and *f*, denoting the number of failed interactions.

The direct trust value is calculated as

$$\frac{S+1}{S+f+2} \qquad (5)$$

Recommendation trust is a special type of direct trust. It is for trust relationship {*subject*: *agent*, *making correct recommendations*}.When the subject can judge whether a recommendation is correct or not, the subject calculates the recommendation trust from s_r and f_r values, where s_r and f_r are the number of good and bad recommendations received from the agent, respectively. This judgment is often done by checking consistency between observations and recommendations, or among multiple recommendations.

The recommendation trust can be calculated as

$$\frac{S_r+1}{Sr+fr+2} \qquad (6)$$

Indirect trust: Trust can transit through third parties. For example, if *A* has established a recommendation trust relationship with *B*, and *B* has established a trust relationship with *Y*, *A* can trust *Y* to a certain degree if *B* tells *A* its trust opinion (i.e., recommendation) of *Y*. This phenomenon is called *trust propagation*. Indirect trust is established through trust propagation.

Two key factors determine indirect trust. The first is when and from whom the subject can collect recommendations. For example, in a sensor network, a sensor may only get recommendations from its neighbors when there is a significant change in their trust records. This affects the number of available recommendations and the overhead of collecting recommendations. The second is to determine how to calculate indirect trust values based on recommendations. When node *B* establishes direct trust in node *Y*, and node *A* establishes recommendation trust in node *B*, *A* – *B* – *Y* is one recommendation path. One recommendation path can contain more than two hops, such as *A* – *B*1 – *B*2 – … – *Y*, and there may be multiple recommendation paths, such as *A* – *B*1 – *Y*, *A* – *B*2 – *Y*, …, and so on. *A trust model determines* how to calculate indirect trust between *A* and *Y* from trust propagation paths. There have been many trust models proposed for various applications [30].

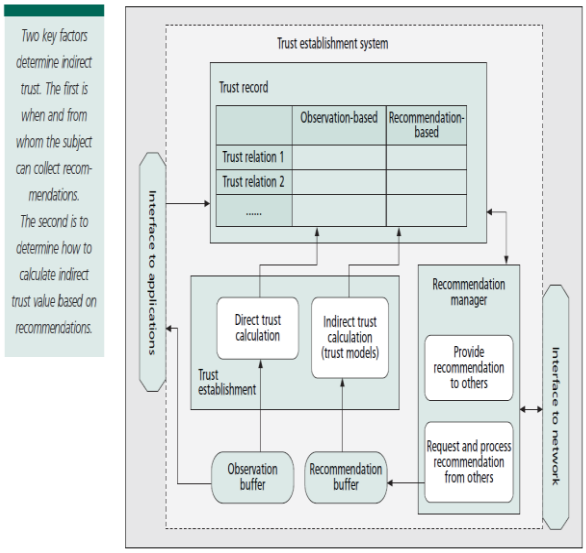

Figure 2: Basic Elements trust establishment systems

3.3. Lightweight Scheme for Trust Decision-making

Our proposed trust decision-making scheme facilitates based on a lightweight scheme. By closely considering the identities of nodes in clustered WSNs, this scheme reduces risk and improves system efficiency while solving the trust evaluation problem when direct evidence is insufficient.

This scheme is described as follows:

3.3.1 Trust Decision-Making at CM Level

A CM calculates the trust value of its neighbors based on two information sources (Fig.3): direct observations (or direct trust degree, DTD) and indirect feedback (or indirect trust degree, ITD). DTD is evaluated by the number of successful and unsuccessful interactions. In this work, interaction refers to the cooperation of two CMs. All CMs communicate via a shared bidirectional wireless channel. If node x sends a message to CH i via node y, then node x can hear whether node y forwarded such message to CH i, the destination. If x does not overhear the retransmission of the packet within a threshold time from its neighboring node y or if the overheard packet is found to be illegally fabricated (by comparing the payload that is attached to the packet), then will consider the interaction unsuccessful. This indirect feedback mechanism has numerous advantages such as the effective mitigation of the effect of malicious feedback, thereby reducing the networking risk in an open or hostile WSN environment and improving system resource efficiency. As an example of trust decision-making at the CM level, if a node x wants to communicate with node y, x first checks whether it has any past interaction records with y during a specific time interval. If a past interaction record exists, then x makes a decision directly; otherwise, x will send a feedback request to its CH.

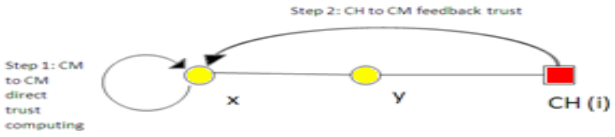

Figure 3: Trust decision-making at CM level.

3.3.2 Trust Decision-Making at CH Level

In cluster WSNs, CHs can forward the aggregated data to the central BS through other CHs. Thus, the selection of CHs is a very important step for dependable communication. In our Trust scheme, CH is evaluated by two information sources (Fig. 4): *CH-to-CH d*irect trust and *BS-to-CH* feedback trust. During *CH-to-CH* communication, the CH maintains the records of past interactions of another CH in the same manner as CMs keep interaction records of their neighbors. Thus, the direct trust value can be computed according to the number of successful and unsuccessful interactions. The BS periodically asks all CHs for their trust ratings on their neighbors. After obtaining the ratings from CHs, the BS will aggregate them to form an effective value of ITD. The ITD of a CH only depends on the feedback reported by the BS. Thus, in the CH-to-CH communication case, when a CH i want to interact with another CH j, it will send a feedback request to the BS, at the maximum. Therefore, including the response message from the BS, the total communication overhead is two packets. Thus, this mechanism can also greatly reduce network communication overhead and improve the system's resource efficiency. As an example of trust decision-making at the CH level, if a CH i want to communicate with another CH j, i first calculate CH-to-CH direct trust for based on the past interaction records with j during a specific time interval. Meanwhile, i send a feedback request to the BS. After receiving the request, the BS will send a response message to i, in which j's feedback trust value (BS-to-CH feedback trust) is embedded. Then, i will aggregate these trust sources into a GTD, after which i will make a final decision based on j's GTD.

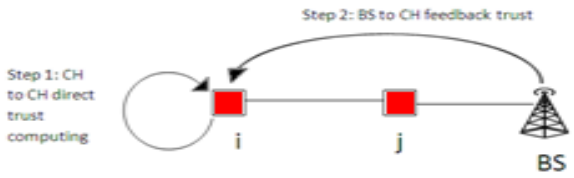

Figure 4: Trust decision-making at CH level.

2. Summary of Trust Relationships

As shown in Figs. 3 and 4, Trust scheme needs to maintain two levels of trust: inter cluster trust and intra cluster trust. Intra cluster trust evaluation has two kinds of trust relationship: *CM-to-CM* direct trust and *CH-to-CM* feedback trust. Likewise, inter cluster trust evaluation also has two kinds of trust relationship, *CH-to-CH* direct trust and *BS-to-CH* feedback trust.

3. Performance Evaluation

To evaluate the performance, we simulated our scheme. We consider that sensor nodes are randomly placed over the two-dimensional field with following assumptions:

• The sensor nodes are mobile but the sink is immobile outside of the network field.

• The sensor nodes with global positioning system (GPS) devices can be aware of their location using a localization mechanism [20] and exchange their information with their neighbors periodically.

• They can aware the speed, movement direction and the amount of their residual energy.

• All nodes have identical processing and communication capabilities.

Figure 5 represents a result of simulations where rounds 90% nodes alive. Figure 5 demonstrates that the sensor nodes in proposed scheme survived longer than the other clustering schemes. In Figure 5, the *x*-axis represents the number of nodes alive per round and the *y*-axis represents the simulation time. LEACH selects the cluster heads without considering the location of the sensor nodes. In M LEACH slowly moving node is likely to be selected as a cluster head. The proposed scheme can prolong the network lifetime because the distance between cluster head and their members is small due to the consideration of density so consumes less energy for transmitting and receiving the data. Therefore our scheme is more effective scheme in terms of prolonging the sensor node lifetime, which is one of the most important factors in wireless sensor networks.

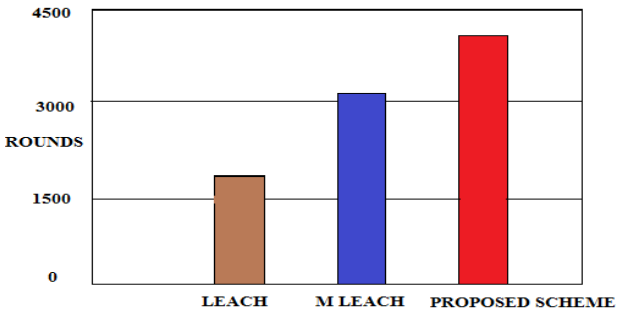

Figure 5: Life time of sensor nodes

Figure 6 shows the leaving rate. The leaving rate is the ratio of nodes which move away from their cluster head before a new cluster head is selected in the next round. As shown in Figure 6, proposed scheme has less leaving rate when compared to existing schemes as cluster head is selected considering the similarity of movement with the member nodes. In M-LEACH, the leaving rate might be increased by selecting a slowly moving node as a cluster head. This result of the simulation also indicates that a proposed scheme is more effective for stable clustering compared to the other schemes.

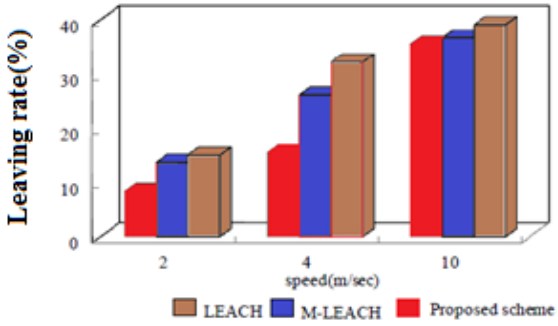

Figure 6: Leaving rate of sensor nodes

4. Overhead Evaluation and Comparison

The comparison results are shown in Fig. 7. With the increasing the number of CMs in a cluster, the CM-to-CM communication overhead of GTMS rapidly increased according to a exponential curve. However, the CM-to-CM communication overhead of LDTS slowly increased with the increasing number of CMs. This finding further confirms that feedback between CMs need not be considered, this trust calculation mechanism can greatly reduce communication overhead.

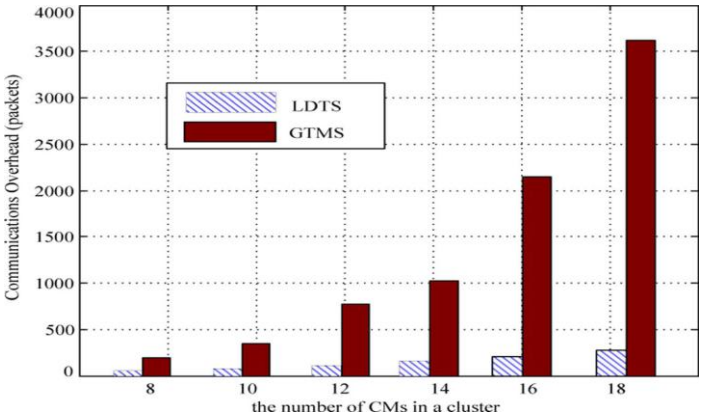

Figure 7: CM-to-CM communication overhead in a cluster.

Fig. 8 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.

However, by comprehensively analyzing the results in Figs. 8 and 9, LDTS is more suitable for large-scale clustered

WSNs with a large size of clusters, thus outperforming GTMS.

Fig. 9 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.

Fig. 10 shows the average storage overhead of the two trust systems at each CH in a WSN network having an equal size of clusters (10 nodes). We find that as the number of clusters increases in the network the GTMS introduces slightly less storage overhead compared with LDTS. Each CH has to maintain an additional table, which is used to store the feedback.

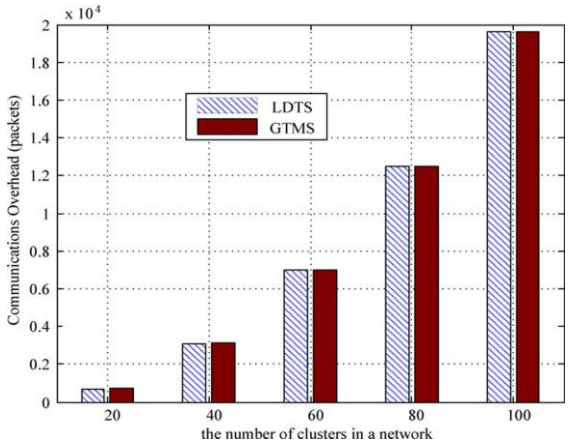

Figure 8: CH-to-CH communication overhead in a network.

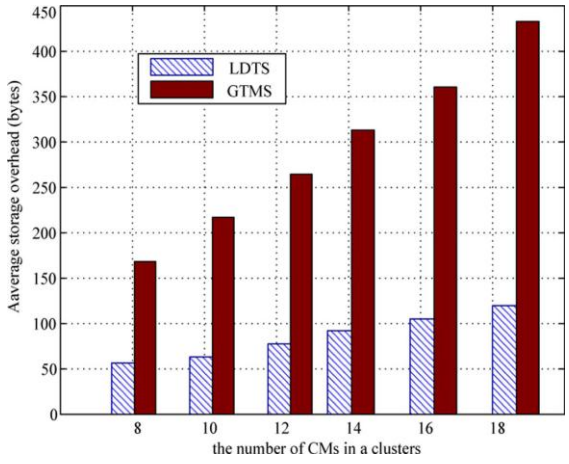

Figure 9: Average storage overhead at each CM in a cluster.

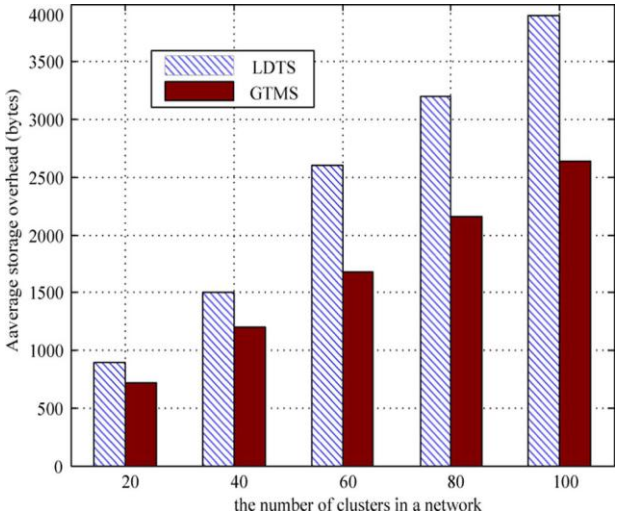

Figure 10: Average storage overhead at each CH in a network.

CONCLUSIONS

In present work we have proposed a clustering scheme considering the mobility with trust dependable system for MWSNS. To select an energy efficient cluster head, we use the following potential score which considers three factors; the similarity of movement, residual energy and density, and link connection time. In addition, lightweight trust decision-making scheme is proposed based on the nodes' identities in the clustered MWSNs.

It facilitates energy-saving by canceling feedback between cluster members (CMs) or between cluster heads (CHs), which is suitable for WSNs. This approach can significantly improve system efficiency while reducing the effect of malicious nodes**.** In conclusion, our scheme obviously increases the life time, dependability and resource efficiency for WSNs as compared with the other scheme. Nonetheless, our scheme still needs to be improved in various conditions and applications. As part of our future work by reducing overhead of the CHs and we will extend our algorithm to enhance its accuracy by diversifying the factors.

REFERENCES

[1] Y. Sun, Z. Han, and K. J. R. Liu, "Defense of trust management vulnerabilities in distributed networks," *IEEE Commun.Mag.*, vol. 46, no. 2, pp. 112–119, Feb. 2009.

[2] R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, and S. Lee, "Group-based trust management scheme for clustered wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 11, pp. 1698–1712, Nov. 2009.

[3] F. Bao, I. Chen,M.Chang, and J. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection," *IEEE Trans. Netw. Service Manag.*, vol. 9, no. 2, pp. 169–183, Jun. 2012.

[4] G. Zhan, W. Shi, and J. Deng, "Design and implementation of TARF:A trust-aware routing framework for WSNs," *IEEE Trans. Depend.Secure Comput.*, vol. 9, no. 2, pp. 184–197, Apr. 2012.

[5] E. Aivaloglou and S. Gritzalis, "Hybrid trust and reputation management for sensor networks," *Wireless Netw.*, vol. 16, no. 5, pp.1493–1510, Jul. 2010.

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

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

[8] Hyunsook Kim, "An Efficient Clustering Scheme for Data Aggregation Considering Mobility in Mobile Wireless Sensor Network", International Journal of Control and Automation Vol. 6, No. 1, February, 2013.
[9] Y. Sun, Z. Han, and K. J. R. Liu, "Defense of trust management vulnerabilities in distributed networks," *IEEE Commun.Mag.*, vol. 46, no. 2, pp. 112–119, Feb. 2009.
10] LDTS: A Lightweight and Dependable Trust System for Clustered Wireless Sensor Networks.
[11] W. Su, S. -J. Lee and M. Gerla, "Mobility Prediction and Routing in Ad hoc Wireless Networks", International Journal of Network Management, vol. 11, no. 1, **(2001)**, pp. 3-30.
[12] T. Taleb, E. Sakhaee, A. Jamalipour, K. Hashimoto, Nei Kato and Yoshiaki Nemoto, "A Stable Routing Protocol to Support ITS Services in VANET Networks", IEEE Transactions on Vehicular Technology, (2007), pp. 3337-3347.