ISSN:2320-0790

compusoft
An International Journal of Advanced Computer Technology

A Trivial and Dependable Faith Scheme for Clustered Wireless Sensor Networks

Ramya. M[1], M.Govindaraj[2]
[1] II M.E (CSE), Dept. of Computer Sci. and Engg, RVS College of Engineering and Technology, Coimbatore, India
[2]Assistant Professor, Dept. of Computer Sci. and Engg. RVS College of Engineering and Technology, Coimbatore, India

Abstract: Wireless Sensor networks (WSN) are a special type of wireless networks. The clustered wireless sensor networks are incapable of satisfying the resource efficiency and dependability of a trust system because of the high overhead and low dependability. A Lightweight and dependable trust system for wireless sensor networks are used to WSNs, which employees the Clustering Algorithm. A lightweight trust decision-making scheme is based on the nodes' identities in the clustered WSNs, which is suitable for such WSNs because it facilitates energy-saving. Due to canceling feedback between cluster members and cluster heads, this approach can significantly improve system efficiency while reducing the effect of malicious nodes. The Cluster heads 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 can effectively reduce the networking consumption and thus prevents malicious, selfish, and faulty Cluster heads. A self-adaptive weighted method is defined for trust aggregation at Cluster head level. Even though this enhances the energy efficiency and confirms the trustworthiness of nodes that participate in the communication. This approach surpasses the limitations of traditional weighting methods for trust factors, in which weights are assigned subjectively. LDTS uses the benefits of an energy-efficient, less memory and communication overhead in wireless sensor networks.

Keywords: Reputation, self-adaptivity, trust management, trust model, wireless sensor network.

I. INTRODUCTION

For Cluster wireless sensor networks (WSNs) such as clustering algorithms can effectively improve network scalability and throughput. Using clustering algorithms, 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. 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 multihop 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 intercluster 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). First, *limited work has focused on the resource efficiency of clustered WSNs.* A trust system should be lightweight to serve a large number of resource-constrained nodes in terms of accuracy, convergence speed, and additional overhead. Furthermore, *limited work has focused on the dependability of the trust system itself.* A trust management system collect remote feedback and then aggregates such feedback to yield the global reputation for the node that can be used to evaluate the global trust degree (GTD) of this node.

II. LITERATURE SURVEY

A universal trust system designed for clustered WSNs to achieve dependability and resource efficiency remains lacking. R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, and S. Lee, [7] proposed GTMS, a group-based trust management scheme for clustered WSNs. GTMS evaluates the trust of a group of nodes in contrast to traditional trust schemes that always focus on the trust values of individual nodes. This approach 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. However, 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. F.Bao, I. Chen, M.Chang, and J. Cho [8] proposed HTMP, a hierarchical dynamic trust management protocol for cluster-based WSNs that considers two aspects of trustworthiness: social trust and QoS (quality-of service) trust. The authors developed a probability model utilizing stochastic Petri net techniques to analyze protocol performance and then validated subjective trust against the objective trust obtained based on ground truth node status. However, implementing such a complex trust evaluation scheme at each CM of the cluster is unrealistic. G. V. Crosby, N. Pissinou, and J.Gadze, [12] 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. A. Boukerche, X. Li, and K. EL-Khatib, [20] 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 [7].

III. LIGHTWEIGHT SCHEME FOR TRUST DECISION-MAKING

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 as collaborative nodes. A node in the clustered WSN model can be identified as a CH or CM (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. We assume that nodes are organized into clusters with the help of a proposed clustering scheme such as [1] and [4]. We assume that all nodes have unique identities, which is similar to the assumptions of [7] and [12]. 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<location, node type, node subtype>. To protect trust values from traffic analysis or fabrication during transfer from one node to another, we also assume a secure communication channel, which can be established by using any key management scheme.

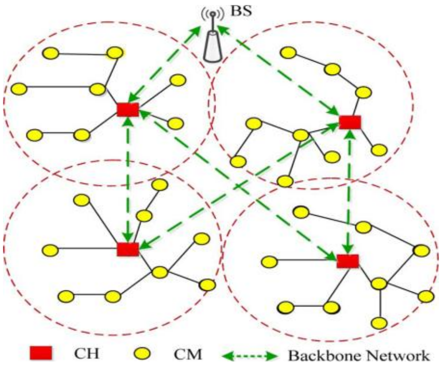


Fig:1. Roles and identities of nodes in a clustered WSN model.

B. Lightweight Scheme for Trust Decision-Making

A LDTS facilitates trust decision-making based on a lightweight scheme. This scheme reduces risk and improves system efficiency while solving the trust evaluation problem. This scheme is described as follows:

(1)*Trust Decision-Making at CM Level:* A CM calculates the trust value of its neighbors based on two information sources (Fig. 2): 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 and operate in the promiscuous mode, that is, if node sends a message to CH via node, then node can hear weather node forwarded such message to CH, the destination. 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 consider the interaction unsuccessful.

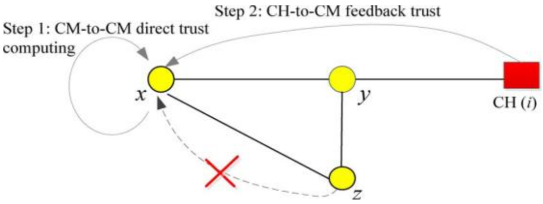

Step 1: CM-to-CM direct trust computing
Step 2: CH-to-CM feedback trust
x
y
z
CH (i)

Fig. 2. Trust decision-making at CM level.

2) Trust Decision-Making at CH Level: In cluster WSNs, CHs form a virtual backbone for inter-cluster routing where 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 LDTS, the GTD of a CH is evaluated by two information sources (Fig. 3): *CH-to-CH* direct 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

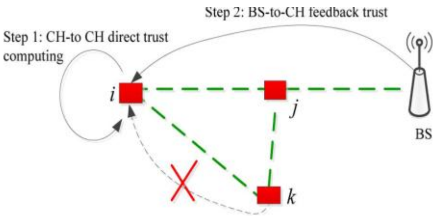

Step 1: CH-to CH direct trust computing
Step 2: BS-to-CH feedback trust
i
j
k
BS

Fig. 3. Trust decision-making at CH level.

IV. LIGHTWEIGHT AND DEPENDABILITY-ENHANCED TRUST CALCULATION

A.Domain of Trust Values

The trust relationship is generally expressed as a specific quantitative value. This value can be a real number between 0 and 1 or an integer between 0 and 100 (e.g., [8]). In this work, we transform this value into an unsigned integer in the interval between 0 and 10.

B. Intra-cluster Trust Evaluation

1) CM-to-CM Direct Trust Calculation: The trust evaluation approach at CMs is defined by the following equation:

$$Tx,y(\Delta t) = \left[\left(\frac{10 \times Sx,y(\Delta t)}{Sx,y(\Delta t) + Ux,y(\Delta t)}\right)\left(\frac{1}{\sqrt{Ux,y(\Delta t)}}\right)\right]$$

2) 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, will maintain these trust values in a matrix H, as shown below:

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

C. Dependability-Enhanced Inter-cluster 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. In LDTS, we propose a dependable and energy-saving scheme, which is suitable for large-scale and clustered WSNs.

1) 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 *i* toward another CH *j* is defined as:

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

2) BS-to-CH Feedback Trust Calculation: Supposing that *m* 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 $\mathcal{B}$, as shown below:

$$\mathcal{B} = \begin{pmatrix} \mathcal{C}_{1,1} & \mathcal{C}_{1,2} & \cdots & \mathcal{C}_{1,m} \\ \mathcal{C}_{2,1} & \mathcal{C}_{2,2} & \cdots & \mathcal{C}_{2,m} \\ & & \ddots & \\ \mathcal{C}_{m,1} & \mathcal{C}_{m,2} & \cdots & \mathcal{C}_{m,m} \end{pmatrix}$$

3) Self-Adaptive Global Trust Aggregation at CHs: We adopt the idea that the GTD of a CH comprises two parts: the first hand trust (*CH-to-CH* direct trust) and the second hand trust (BS-to-CH feedback trust).Thus, the CH j's GTD is aggregated by the following equation:

$$O_{i,j}(\Delta t) = \lceil 10 \times (w_1 \times \mathcal{C}_{i,j}(\Delta t) + w_2 \times \mathcal{F}_{i,j}(\Delta t)) \rceil$$

D. Dependability Analysis against Malicious Attacks

In clustered WSNs, the main attacks from a malicious node primarily include two kinds of patterns:

1) *Garnished attack*. In such an attack, malicious nodes behave well and badly alternatively with the aim of remaining undetected while causing damage. For instance, garnished malicious nodes may suddenly conduct attacks as they accumulate higher trustworthiness.

2) *Bad mouthing attack*. As long as feedback is considered, malicious nodes can provide dishonest feedback to frame good parties and/or boost trust values of malicious nodes. This attack, referred to as the bad mouthing attack, is the most straightforward attack.

Theorem 1: In the *CM-to-CM* direct trust decision-making at CMs, the proposed LDTS is dependable against the deceptive behavior of malicious CMs.

Proof: Suppose, on the contrary, that a malicious CM *y* for a CM *x* that successfully deceived. Then, according to the Definitions 1 and 2:Ux,y>Sx,y and Tx,y(Δt)≥5 . Three cases can be considered.

1.If Sx,y≥1 , CM *y* has interacted with a CM *x* within the time stamp t. Let *a* denote the real number Ux,y/Sx, y.Given that Ux,y >Sx,y ,we can derivea≥1. Hence, given thatUx,y+Sx,y≠0, at the time of the last interaction, the trust calculation can be performed by using the past interaction evaluation, according to (1):

$$\begin{aligned} \mathcal{T}_{x,y}(\Delta t) &= \left(\frac{10 \times s_{x,y}}{s_{x,y} + u_{x,y}}\right)\left(\frac{1}{\sqrt{u_{x,y}}}\right) \\ &= \left(\frac{\frac{10 \times s_{x,y}}{s_{x,y}}}{\frac{s_{x,y}}{s_{x,y}} + \frac{u_{x,y}}{s_{x,y}}}\right)\left(\frac{1}{\sqrt{u_{x,y}}}\right) \\ &= \left(\frac{10}{1+a}\right)\left(\frac{1}{\sqrt{u_{x,y}}}\right), \quad a = \frac{u_{x,y}}{s_{x,y}} \\ &= \left(\frac{10}{1+a}\right)\left(\frac{\frac{\sqrt{u_{x,y}}}{s_{x,y}}}{a}\right) = \frac{10\sqrt{u_{x,y}}}{s_{x,y}(1+a)a}. \end{aligned}$$

Given that Sx,y≥1 and Ux,y>Sx,y, we obtain

$$u_{x,y} > 1 \Rightarrow \sqrt{u_{x,y}} > 1.$$

Given that Tx,y(Δt)≥5, we obtain

$$5 \leq \frac{10\sqrt{u_{x,y}}}{s_{x,y}(1+a)a} < \frac{10}{s_{x,y}(1+a)a}$$

Which implies that Sx,y(1+a)a<2. Since Sx,y≥1, a≥1 and (a+1) ≥ 2, which is obviously impossible and yields the contradiction Sx,y(1+a)a<2.

(2) If Sx,y=0. We consider Ux,y≥1. Given that Ux,y+Sx,y≠0, at the time of the last interaction, the trust calculation can be performed by using the past interaction evaluation, according to (1):

$$\begin{aligned} \mathcal{T}_{x,y}(\Delta t) &= \left(\frac{10 \times s_{x,y}}{s_{x,y} + u_{x,y}}\right)\left(\frac{1}{\sqrt{u_{x,y}}}\right) \\ &= \left(\frac{10 \times 0}{0 + u_{x,y}}\right)\left(\frac{1}{\sqrt{u_{x,y}}}\right) = 0 \end{aligned}$$

Apparently, this condition contradicts the hypothesis Tx,y(Δt)≥5, which proves Theorem 1.

(3) If Sx,y=0 and Ux,y=0 , CM *y* has no interaction with CM *x* at all within the time. In such case, *x* will rely on the feedback reported by the CH.

V.EXPERIMENTAL RESULTS

A.LDTS Simulator

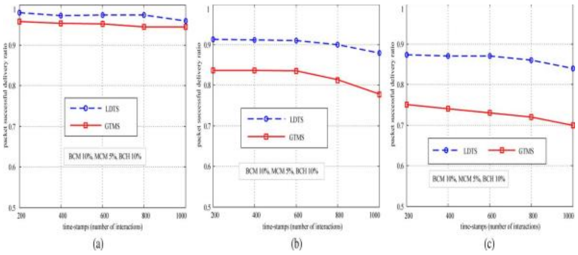
In the simulator, three kinds of nodes exist based on their identities, i.e., as a CM, as a CH, and as a BS. A CM or a CH can be a collaborator or a rater toward other nodes. The behavior of a CM as a rater can be one of two types: honest CM (HCM) and malicious CM (MCM). An HCM always gives the appropriate rating for any CM, whereas an MCM always gives a random rating between 0 and 10 for other CMs.

B .Overhead Evaluation

We aim to study the effect of the trust management system in a WSN community, which closely resembles a real network environment. We suppose that most CMs and CHs are good, where only 20% CMs and CHs are malicious.

VI PERFORMANCE ANALIYSIS

LDTS has a robust performance under dishonest WSN environment.



We find that LDTS also has a more robust dependability than the GTMS scheme. Both LDTS and GTMS have relatively stable performance within 1,000time-steps, even if their trust system changes from 0.92 to 0.96.

VII. CONCLUSION

In this work, we proposed LDTS for clustered WSNs. Given the cancellation of feedback between nodes, LDTS can greatly improve system efficiency while reducing the effect of malicious nodes. By adopting a dependability-enhanced trust evaluating approach for co-operations between CHs, LDTS can effectively detect and prevent malicious, selfish, and faulty CHs. Theory as well as simulation results show that LDTS demands less memory and communication overhead as compared with other typical trust systems and is more suitable for clustered WSNs.

VII. REFERENCES

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

[2] D. Kumar, T. C. Aseri, and R. B. Patel, “EEHC: Energy efficient heterogeneous clustered scheme for wireless sensor networks, Comput.Commun” vol. 32, no. 4, pp. 662–667, Apr. 2009.

[3] Y. Jin, S. Vural, K. Moessner, and R. Tafazolli, “An energy-efficient clustering solution for wireless sensor networks,” *IEEE Trans.Wireless Commun.*, vol. 10, no. 11, pp. 3973–3983, Nov. 2011.[4] O. Younis and S. Fahmy, “HEED: A hybrid, energy-efficient, distributed clustering approach for Ad-Hoc sensor networks,” *IEEE Trans. Mobile Comput.*, vol. 3, no. 4, pp. 366–379, Oct. 2004.

[5] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, “Reputation-based framework for high integrity sensor networks,” *ACM Trans. Sensor Netw*, vol. 4, no. 3, pp. 1–37, May 2008.

[6] 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. [7] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, “A survey of trust and reputation management systems in wireless communications,” *Proc. IEEE*, vol. 98, no. 10, pp. 1752–1754, Oct. 2010.

[7] 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.

[8] 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.

[9] 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.

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

[11] A.Rezgui and M. Eltoweissy, “A reliable adaptive service driven efficient routing protocol suite for sensor-actuator networks,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 5, pp. 607–622, May 2009.

[12] 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.

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