Indian Journal of Emerging Electronics in Computer Communications, Vol.1, Issue 2, Dec 2014, ISSN: 2393-8366

Trust Management in Clustered Wireless Sensor Network

Iqbal Thayyabunisa Begum, K.Lakshmipriya, A.G. Merlyn Beulah, D. Shiny Irene

Abstract— The resource efficiency and dependability of a trust system are the most fundamental requirements for any wireless sensor network (WSN). However, existing trust systems developed for WSNs are incapable of satisfying these requirements because of their high overhead and low dependability. In this work, we proposed a lightweight and dependable trust system (LDTS) for WSNs, which employ clustering algorithms. 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. Due to canceling feedback between cluster members (CMs) or between cluster heads (CHs), this approach can significantly improve system efficiency while reducing the effect of malicious nodes .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 can effectively reduce networking consumption while malicious, selfish, and faulty CHs. Moreover, self adaptive weighted method is defined for trust aggregation at CH level. 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 LDTS demands less memory and communication overhead compared with the current typical trust system for WSNs.

Index Terms—Reputation, self-adaptively, trust management, trust model ,Wireless sensor network.

1. INTRODUCTION

The resource efficiency and dependability of a trust system should undoubtedly the most fundamental requirements for any WSN (including clustered WSNs). However, existing trust systems developed for clustered WSNs are incapable of satisfying these requirements because of their high overhead and low dependability. A universal trust system designed for clustered WSNs for the simultaneous achievement of resource efficiency and dependability remains lacking. First, limited work focus on resources efficiency 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. Based on an integrated comparison, a number of innovative works have been developed for clustered WSNs, such as GTMS, TCHEM , HTMP , ATRM . However, most these works failed to consider the problem of resource constraints of nodes or used complex algorithms to calculate nodes' trustworthiness. Implementing complex trust evaluation algorithms at each CM or CH is unrealistic. Although GTMS uses several novel mechanisms to improve the resource efficiency of clustered WSNs, this approach relies on a broadcast-based strategy to collect feedback among CMs, which requires a significant amount of resource and power To the best of our knowledge, we are the first to conduct a systematic study of a trust management system for clustered WSNs from the perspective of both dependability and resource A lightweight trust evaluating scheme for co operations between CMs or between CHs. Within the cluster, the indirect trust of a CM is evaluated by its CH. Thus each CM does not need to maintain the feedback from other CMs, which will reduce the communication overhead and eliminate the possibility of a bad-mouthing attack by compromised CMs. The feedback of a CH is applied a similar manner to obtain the same benefits. A dependability-enhanced trust evaluating approach for co operations between CHs. 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 can effectively reduce networking consumption while preventing malicious, selfish, and faulty CHs.

A self- adaptive weighting method for CH’s trust aggregation. This approach overcomes the limitations of traditional weighting methods for trust factors, in which weights are assigned subjectively efficiency. The key features of LDTS go beyond existing approaches in terms of the following aspects:

2. RELATED WORK

Research on trust management systems for WSNs received considerable attention from scholars. A number of studies have proposed such systems for 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 .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. proposed HTMP, a hierarchical dynamic trust management protocol for cluster-based WSNs that considers two aspects of trustworthiness: social trust and (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.

LIGHTWEIGHT SCHEME FOR TRUST DECISION-MAKING.

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.

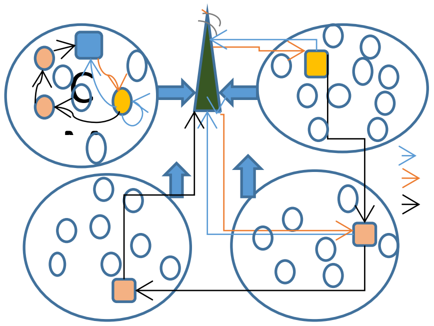
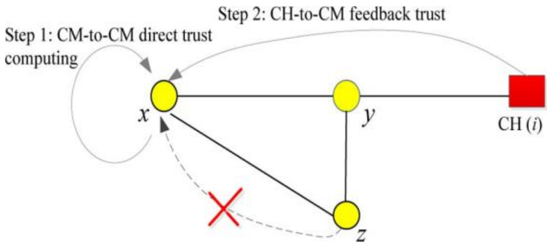


Fig. 1. Roles and identities of nodes in a clustered WSN model.

Our proposed LDTS facilitates trust decision-making 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.

Trust Decision-Making at CM Level*:* ACM 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 wether 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. Unlike most existing reputation or trust models, which rely on broadcast based strategy to collect feedback from the whole cluster, consequently increasing the system communication overhead significantly, our LDTS does not utilize a broadcast- based strategy and instead sets the value of ITD is based on the feedback reported by the CH about a specific node.


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

Thus, each CM does not need to share trust information with its neighbors. 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. Given that the feedback between CMs need not be considered, this mechanism can significantly reduce network communication overhead, thus improving system resource efficiency. As an example of trust decision-making at the CM level, if a node wants to communicate with node , first checks whether it has any past interaction records with during a specific time interval. If a past interaction record exists, then makes a decision directly; otherwise, will send a feedback request to its CH.

LIGHTWEIGHT AND DEPENDABILITY-ENHANCED TRUST CALCULATION

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 . In this work, we transform this value into an unsigned integer in the interval between 0 and 10. Although presenting the trust values as a real number or an integer may be insignificant in traditional networks, this issue is of critical importance for WSNs because of limited memory as well as transmission and reception power this domain of trust values has the following benefits. Less memory overhead. An unsigned integer between 0 and 10 only needs 4 bits (0.5 bytes) of memory space, thus saving save 50%memory space compared with trust values represented as an integer between 0 and 100 (1 bytes) and 87.5% compared with trust values represented as a real number (4 bytes). Less transmission overhead. Given that a smaller number of bits require transmission during the exchange of trust values between nodes, we gain the benefit of less overhead of transmission and reception power.

Dependability-Enhanced Intercluster Trust Evaluation

In accordance with the characteristics of clustered WSNs, both CMs and CHs are resource-constrained nodes, and BSs havemore 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 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: where . is the total number of successful interactions of CH with CH during time window , and is the total number of unsuccessful interactions of CH with CH . BS-to-CH Feedback Trust Calculation*:* Supposing that CHs exist in the network. The base station 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 . will maintain these trust values in a matrix , as shown below: where is the direct trust of CH toward CH . Moreover, , 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 *B*S-to-CH feedback trust is the question of malicious feedback. In [28], Liang and Shi found that the lightweight average aggregation algorithm performs better than complex algorithms, especially when a considerable number of bad raters exist in the system. Inspired by, we use an enhanced beta probability density function to compute for *BS-to*-CH feedback trust.

Storage Overhead Analysis and Comparison

Each CM has to maintain a small trust database, as shown in Fig. . The size of each record is 7 bytes. Therefore, the storage requirement for LDTS at each CM is 7(η-1) bytes, where (η-1) represents the number of CMs in a cluster. The size of the trust table mainly depends on the size of the cluster. Each CH maintains two tables, one of which is used to store the feedback matrix , thus resulting in a total storage overhead of . In the second table, each CH maintains a trust database as shown in. The size of each record also is 7 bytes. Therefore, storage requirement for CHs is bytes, where represents the number of CMs in a cluster.

LDTS Simulator and Environment

In the simulator, three kinds of nodes exist based on their identities (Table III), 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 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. Based on discussions in Section   we can see that LDTS 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 LDTS, in this simulator, we separately evaluate the performance of LDTS 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. Instead of using the physical running time, we use the notion of time-step, which is introduced in Net logo, to calculate the simulation time. The simulation parameters and default values used in the experiments are listed.

Overhead Evaluation and Comparison

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. The comparison results are shown in Fig. 10. With the increasing the 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. This finding further confirms our conclusions from the theoretical analysis in Section VI, that is, given that feedback between CMs need not be considered, this trust calculation mechanism in LDTS can greatly reduce communication overhead. 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 LDTS is more suitable for large-scale clustered WSNs with a large size of clusters, thus outperforming GTMS.

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.

REFERENCE

[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 Net., 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.

[8] 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.

[9] 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.

[10] 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.

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

[12] A.Rezgui andM. Eltoweissy, " :Areliable adaptive servicedriven efficient routing protocol suite for sensor-actuator networks," IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 5, pp. 607–622, May

[13] 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.

[14] R. Ferdous, V. Muthukkumarasamy, 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.

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