ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Design of DTS for Clustered Wireless Sensor Networks

Naveen Urs T. R*1, and H. C. Srinivasaiah2

[*1] Department of Telecommunication Engineering (TCE), Dayananda Sagar College of Engineering, Bangalore. India

[2] Professor, Department of TCE, Dayananda Sagar College of Engineering Bangalore, India

urstrnaveen31@gmail.com

Abstract

The dependability of trust system and resource efficiency are the most fundamental requirements for any Wireless Sensor Network (WSN). However, the existing trust systems developed for WSNs are lacking in satisfying these requirements because of their low dependability and high overhead. In this work, we have proposed a 'Dependable Trust System' (DTS) for WSNs, which employ clustering algorithms. First, a dependable trust, decision-making scheme is proposed based on the nodes identity in the clustered WSNs, which is suitable for WSNs because it results in energy saving. Due to deleting of feedback between Cluster Members (CMs) or between Cluster Heads (CHs), this approach can effectively reduce the existence and effects of malicious nodes while significantly improving the system efficiency. More significantly, considering that CHs take on large amounts of data forwarding and communication tasks, a dependability enhanced trust valuating approach is defined for cooperation between CHs. This approach can efficiently reduce network power consumption while malicious, selfish, and faulty CHs, deleted from the network. Moreover, a self-adaptive weighted method is defined for trust calculation at CH level. This approach stands out the limitations of traditional weighting methods for trust factors. Theory as well as simulation results shows that DTS demands less communication overhead and memory compared with the current typical trust systems for WSNs.

Keywords: Dependability, reputation, self-adaptivity, trust management, cluster, trust model, wireless sensor network.

Introduction

For clustered Wireless Sensor Networks (WSNs) such as 'Low Energy Adaptive Clustering Hierarchy' (LEACH) [1, 2], 'Energy Efficient Heterogeneous Clustering' (EEHC) [3], 'Energy Efficient Clustering' (EC) [4], and 'Hybrid Energy Efficient Distribution Hierarchy' (HEED) [5], clustering algorithms can effectively increase network throughput and scalability. Using clustering algorithms, nodes are grouped as clusters, and within each cluster, a node with high computing power is elected as a 'Cluster Head' (CH). CHs unitedly form a higher level backbone network. After many recursive iterations, a clustering algorithm builds a multilevel WSN structure. This structure facilitates communication and enables the restriction of bandwidth using up network operations such as flooding only to the intended clusters [6]. Building trust in a clustered environment results in numerous advantages, such as enabling a CH to detect malicious or faulty nodes within a cluster [7]. In the case of multihop clustering [5], a trust system helps 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 helps 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) [8].

Motivation

The dependability of trust system and resource efficiency should undoubtedly be the most fundamental requirements for any WSN. However, existing trust systems developed for clustered WSNs are lacking in satisfying these requirements because of their low dependability and high overhead. A universal trust system designed for clustered WSNs for the simultaneous accomplishment of dependability and resource efficiency remains lacking.

First, limited work has focussed on the resource efficiency of clustered WSNs. A trust system should be simple and serve a large number of resource-constrained nodes in terms of convergence speed, accuracy, and additional overhead [9, 10, 11]. Based on an integrated comparison, a number of innovative works have been developed for clustered WSNs, such

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

as Group Based Trust Management Scheme (GTMS) [9], Hierarchical Dynamic Trust Management Protocol (HTMP) [1]. However, most of these works failed to consider the problem of resource constraints of nodes or they have used complex algorithms to calculate nodes' trustworthiness. Applying complex trust evaluation algorithms at each CM or CH is unrealistic. Although GTMS uses several novel mechanisms to increase 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.

Furthermore, limited work has focussed on the dependability of the trust system itself. In existing trust calculations for WSNs, trust management systems receives 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. However, an open or unfriendly WSN environment contains a large number of undependable or faulty nodes. Feedback from these undependable nodes may yield wrong evaluation. The dependability of a trust system is undoubtedly an important requirement for any WSN. That is, a trust system should be highly dependable in terms of providing service in an open or unfriendly WSN environment. However, most previous algorithms lack feasible alternatives to solve the problem of malicious feedback, which significantly affects system feedback availability and dependability. Recent studies for clustered WSNs (e.g., HTMP [1]), the authors follow simple weighted average approaches to aggregate feedback trust information without considering the problem of malicious feedback. This may result in misjudgement of the trust decision making process.

Objective

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 view of both resource efficiency and dependability. The key features of DTS go beyond existing approaches in terms of the following aspects:

1. *A lightweight trust measuring scheme for cooperation between CMs or between CHs*. Within the cluster, the indirect trust of a CM is measured by its CH. Thus each CM does not need to maintain the feedback from other CMs, which will decrease the communication overhead and eliminate the possibility of a bad-mouthing attack by compromised CMs. The feedback of a CH is applied in a similar way to obtain the same benefits.
2. *A dependability enhanced trust measuring approach for cooperation between CHs*. Considering that CHs take on large amounts of data forwarding and communication tasks, a dependability enhanced trust measuring approach is defined for cooperation between CHs. This approach can effectively reduce networking consumption while avoiding malicious, selfish, and faulty CHs.
3. *A self-adaptive weighting method for CH's trust aggregation*. This approach overcomes the limits of traditional weighting methods for trust factors, in which weights are assigned in a subjective manner.

These new designs and other specific features collectively make the DTS a lightweight, self-adaptive, and dependable solution that can be used in any clustered WSN. This paper will provide both theoretical bases and experimental results to validate the designs of the DTS. The remainder of this paper is organized as follows: Section II gives an overview of related work. Section III discusses trust modelling and evaluation mechanism in DTS and provide the theoretical and simulation based analyses and evaluation of DTS. Section IV concludes this paper.

Related work

Research on trust management systems for WSNs received appreciable 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 [9], HTMP [7], and 'Agent-based Trust Reputation Management (ATRM). To our best knowledge, a universal trust system designed for clustered WSNs to achieve resource efficiency and dependability remains lacking.

Shaikh *et al.* [9] proposed GTMS, a group-based trust management scheme for clustered WSNs. It 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 and every node. GTMS helps 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, which requires a significant amount of resources and power.

Bao *et al.* [10] proposed HTMP, a hierarchical dynamic trust management protocol for cluster-based

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

WSNs that considers two aspects of trustworthiness: social trust and QoS trust. The authors developed a probability model utilizing stochastic 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.

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 (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. We assume that nodes are organized into clusters with the help of a proposed clustering scheme.

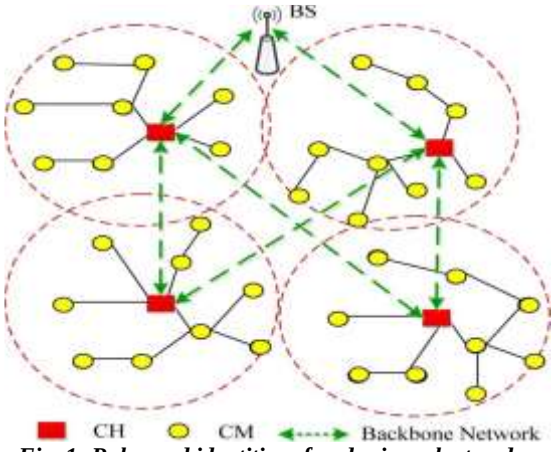

Fig. 1: Roles and identities of nodes in a clustered WSN model.

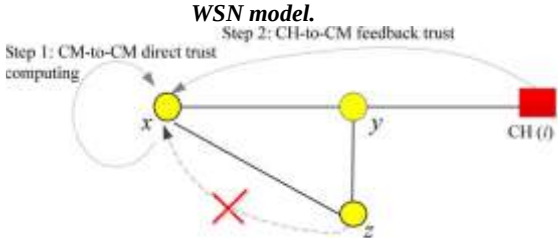

Fig. 2: Trust decision-making at CM level.

We assume that all nodes have unique identities, which is similar to the assumptions of [7, 10, 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. 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.

1. *Trust Decision-Making at CM Level:* A CM calculates the trust value of its neighbours 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 *x* sends a message to CH via node *y*, then node *x* can hear whether node *y* forwarded such message to CH, the destination. If *x* does not overhear the retransmission of the packet within a threshold time from its neighbouring node or if the overheard packet is found to be illegally fabricated (by comparing the payload that is attached to the packet), then *x* will consider the interaction unsuccessful. Unlike most existing reputation or trust schemes, which rely on broadcast-based strategy to collect feedback from the whole cluster, consequently increasing the system communication overhead significantly, our DTS does not utilize a broadcast based strategy and it instead sets the value of ITD based on the feedback reported by the CH about a specific node. Thus, each CM does not need to share trust information with its neighbours. 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 *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 exists, then *x* makes a decision directly; otherwise, *x* will send a feedback request to its CH.
2. *Trust Decision-Making at CH Level:* In cluster WSNs, CHs form a virtual backbone for intercluster 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 DTS, the GTD of a CH is evaluated by two

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

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 neighbours. Thus, the direct trust value can be computed according to the number of successful and unsuccessful interactions. The Base Station periodically asks all CHs for their trust ratings on their neighbours. After obtaining the ratings from CHs, the BS will aggregate them to form an effective value of ITD. Similar to the trust decision-making process at the CM level, in our DTS, 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 wants to interact with another CH, it will send a feedback request to the BS, at the maximum. Therefore, including the response message form the BS, the total communication overhead is two packets. Thus, this mechanism can also greatly reduce network communication overhead and consequently improve the system's efficiency. Compared with trust decision-making at the CM level, trust decision making at the CH level has to calculate for direct trust and feedback trust simultaneously. As an example of trust decision-making at the CH level, if a CH wants to communicate with another CH, first calculates CH-to-CH direct trust for based on the past interaction records with during a specific time interval. Meanwhile, sends a feedback request to the BS. After receiving the request, the BS will send a response message to, in which the feedback trust value (BS-to-CH feedback trust) is embedded. Then, will aggregate these trust sources into a GTD, after which will make a final decision based on GTD.

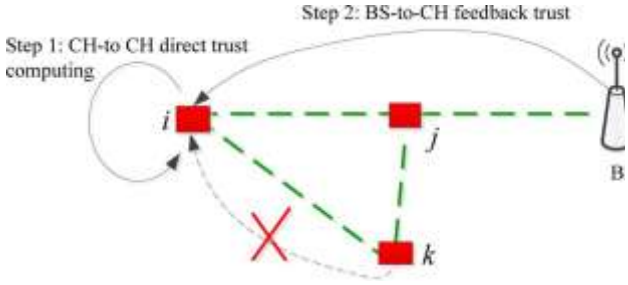

Fig. 3: Trust decision making at CH level.

B. Dependability Analysis Against Malicious Nodes

In this section, we analyze the dependability of the DTS protocol against attacks on a trust management system. 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 is referred to as the bad mouthing attack [7], is the most straightforward attack. After providing evidence of the malicious nodes' objectives, we can prove that our trust management system at both the CM and CH levels is dependable against attacks from malicious nodes because this system can detect the malicious behaviour and can prevent such nodes from fulfilling their objectives. We broadly categorize two types of nodes (CMs or CHs): good ones and malicious ones. Our assumption is that good nodes interact successfully most of the time and submit true feedback. Conversely, malicious nodes try to launch garnished attacks or bad mouthing attacks. We define this concept more rigorously, capture the behaviour of malicious nodes, and model how such nodes might try to gain an unfair advantage in our trust scheme. Then, we prove our trust system's dependability against such malicious attacks.

C. Communication Overhead Analysis and Comparison

To evaluate the communication overhead under full-load conditions, we assume a worst-case scenario which is similar to [9], 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 CM, and the BS has to collect feedback reports from its CH. Let us assume that the network consists of m clusters and that the average size of clusters is n (including the CH of the cluster). In intracluster trust evaluation, when node *x* wants to interact with node *y*, node *x* will send a maximum of one CH feedback request, for which node *y* will receive one response. If node *x* wants to interact with all the nodes in the cluster, the maximum communication overhead will be *2(n-2)*. If all nodes want to communicate with one another, the maximum communication overhead is *2(n-2)(n-1)*. When a CH wants to collect feedback from its *n* members, it will send *n* requests and receive *n* responses, thus resulting in a total communication overhead of *2n*. Thus, the maximum intracluster communication overhead is $C_{intra} = 2(n-2)(n-1)+2n$. In the intercluster

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

communication case, when *CH i* want to interact with *CH j*, it will send one BS feedback request to the BS, at the maximum. Thus, the communication overhead is two packets. If *CH i* want to communicate with all the CHs, then the maximum communication overhead will be *2(m-1)* packets. If all the CHs want to communicate with one another, the maximum communication overhead is $2(m-1)(m-1) = 2(m-1)^2$. When the BS wants to collect feedback from its *m* CHs, it will send requests and receive *m* responses, thus resulting in a total communication overhead of *2m*. Thus, the maximum intercluster communication overhead is $C_{inter} = 2(m-1)^2+2m$. Therefore, the maximum communication overhead introduced by the DTS to the entire network is:

$C_{max}=m\times C_{intra}+C_{inter}=2m\ [(n-2)(n-1)+n] + 2(m-1)^2+2m$

Fig. 4 shows the plot of communication overhead as a function of number of nodes. It's clear from the plot that, the communication overhead depends only on the number of nodes present in each cluster. As the number of nodes increases, the overhead due to communication increases. Since in our DTS scheme we have a strategy of deleting or avoiding the communication via malicious nodes, it results in decreased communication overhead. Here we calculate the overhead as intra and inter cluster and finally we calculate the maximum overhead of the network.

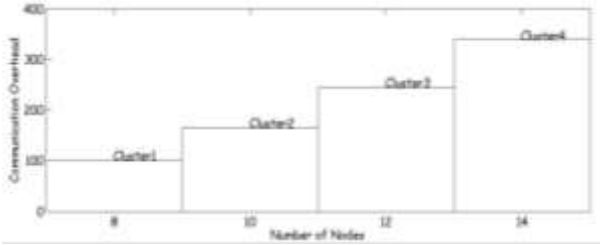

Fig. 4: Communication overhead versus number of nodes.

D. Storage Overhead Analysis and Comparison

Each CM has to maintain a small trust database; the size of each record is 7 bytes. Therefore, the storage requirement for DTS at each CM is *7(n-1)* bytes, where *(n-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 $0.5(n-1)^2$. In the second table, each CH maintains a trust database. The size of each record also is 7 bytes. Therefore, storage requirement for m CHs is *7(m-1)* bytes, where *(m-1)* represents the number of CMs in a cluster. The total storage overhead at the CH for both tables is $C_{m\text{-}max} = 7(m-1) + 0.5(m-1)(n-1)^2$.

Table I: Analysis and comparison of storage requirements for DTS, GTMS, and ATRM

Models	*CM Nodes*	*CH Nodes*
DTS	$7(n-1)$	$7(m-1)+0.5m(n-1)^2$
GTMS	$(n-1)(4+4\Delta t)$	$(m+n-2)(4+4\Delta t)$
ATRM	$30n+8(k-1)$	$30(m+n)+2(4k-19)$

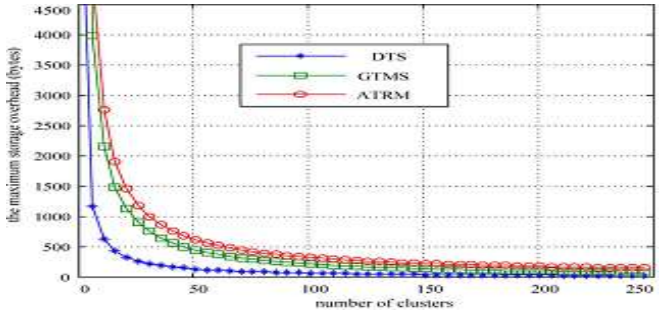

Fig. 5: Storage overhead at each CM with 1,000 nodes.

The formulas for the storage requirements of three trust management systems DTS, GTMS, and ATRM, are given in Table I, in which *n* represents the average number of CMs in each cluster, *m* represents the total number of CHs in the network, *t* is the time window defined by GTMS, and *k* represents the number of contexts described in ATRM. Fig. 5 shows the storage overhead of three trust management systems under a clustered WSN environment, which has a total of 1,000 nodes. On the whole, in the curves of Fig. 5, we can see that our DTS needs less storage overhead than the two other systems, i.e. GTMS and ATRM. This condition proves that DTS at the CM level consumes less memory than the two other models.

E. 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. 6. With the increasing the number of CMs in a cluster, the CM-to-CM communication overhead of GTMS rapidly increased exponentially. However, the CM-to-CM communication overhead of DTS is slowly increased with the increasing number of CMs, in comparison with GTMS. Fig. 7 shows the comparison results of the CH-to-CH communication overhead between DTS and GTMS. DTS and GTMS have a relatively larger difference in network overhead when the number of nodes are around 18 and below. The comprehensive analysis of the results in Figs. 6 and 7, shows that the DTS is more suitable for large-scale clustered WSNs with a large size of clusters, thus outperforming GTMS.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

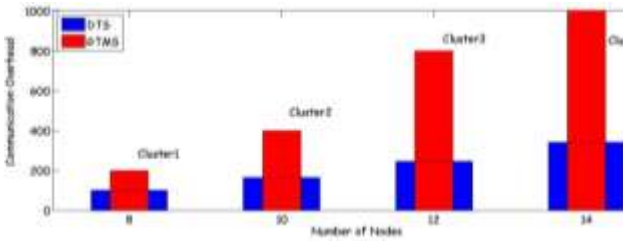

Fig. 6: CM-to-CM communication overhead in a cluster.

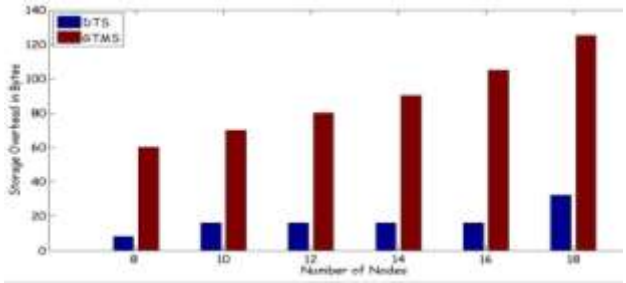

Fig. 7: CH-to-CH communication overhead in a network.

Conclusion

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

Acknowledgement

Authors would like to acknowledge Management, Dayananda Sagar Group of Institutions (DSI), Bangalore, India for all its support and constant encouragement for this project work.

References

1. *Xiaoyong Li, Feng Zhou, and Junping Du, "LDTS: A Lightweight and Dependable Trust System for Clustered Wireless Sensor Networks", IEEE Transactions on Information Forensics and Security, Vol. 8, No. 6, June 2013, pp. 924-935.*
2. *W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application- specific protocol architecture for wireless microsensor networks," IEEE Transaction Wireless Commun., vol. 1, no. 4, pp. 660–670, Oct. 2002.*
3. *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.*
4. *Y. Jin, S. Vural, K. Moessner, and R. Tafazolli, "An energy-efficient clustering solution for wireless sensor networks," IEEE TransactionWireless Commun., vol. 10, no. 11, pp. 3973–3983, Nov. 2011.*
5. *O. Younis and S. Fahmy, "HEED: A hybrid, energy-efficient, distributed clustering approach for Ad-Hoc sensor networks," IEEE Transaction Mobile Comput., vol. 3, no. 4, pp. 366–379, Oct. 2004.*
6. *S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," ACM Transaction Sensor Netw., vol. 4, no. 3, pp. 1–37, May 2008.*
7. *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.*
8. *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.*
9. *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 Transaction Parallel Distrib. Syst., vol. 20, no. 11, pp. 1698–1712, Nov. 2009.*
10. *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 Transaction Network Service Management, vol. 9, no. 2, pp. 169–183, Jun. 2012.*
11. *G. Zhan, W. Shi, and J. Deng, "Design and implementation of TARF: A trust-aware routing framework for WSNs," IEEE Transaction Depend. Secure Compuer, vol. 9, no. 2, pp. 184–197, Apr. 2012.*
12. *Aivaloglou and S. Gritzalis, "Hybrid trust and reputation management for sensor networks," Wireless Netw., vol. 16, no. 5, pp. 1493–1510, Jul. 2010.*
13. *A. Rezgui and M. Eltoweissy, "A reliable adaptive service driven efficient routing protocol suite for sensor-actuator networks," IEEE Transaction Parallel Distribution Sysetem, vol. 20, no. 5, pp. 607–622, May 2000.*