Trust framework for a secured routing in wireless sensor network

Ouassila HOCEINI,
Laboratoire LARI, Université Mouloud Mammeri de Tizi Ouzou, Algerie
ouassila.hoceini@gmail.com

Said TALBI,
Laboratoire LMCS, Ecole nationale supérieure d'informatique (ESI), Alger, Algérie
Said.talbi@yahoo.fr

Rachida AOUDJIT
Laboratoire LARI, Université Mouloud Mammeri de Tizi Ouzou, Algerie
rachida_aoudjit@yahoo.com

Résumé

Les techniques traditionnelles développées pour éliminer les attaques internes dans les réseaux filaires et sans fils ne sont pas adéquates pour les réseaux de capteurs, vu les contraintes de ressources. Afin de protéger les réseaux de capteurs sans fils (RCSF) contre les fait malicieux et égoïstes, quelques systèmes basés confiance sont récemment modélisés. L'efficacité et la fiabilité des ressources d'un système de confiance sont les besoins les plus fondamentales pour n'importe quel réseau de capteurs.

Dans ce papier, nous avons proposé une architecture de confiance pour un routage sécurisé dans un réseau de capteurs sans fils, qui emploie une topologie hiérarchique. Cette approche peut réduire considérablement le coût d'évaluation de la confiance et garantit une meilleure sélection de chemins sécurisés qui mènent vers la station de base. La théorie et les résultats de simulation montrent que notre schéma utilise moins de ressources et d'énergie comparé aux systèmes de confiance actuels dans les réseaux de capteurs sans fils. De plus, il détecte les noeuds malicieux et défectifs et nous protège des attaques internes.

Abstract

Traditional techniques to eliminate insider attacks developed for wired and wireless ad hoc networks are not well suited for wireless sensors networks due to their resource constraints nature. In order to protect WSNs against malicious and selfish behavior, some trust-based systems have recently been modeled. The resource efficiency and dependability of a trust system are the most fundamental requirements for any wireless sensor network (WSN).

In this paper, we propose a Trust Framework for a Secured Routing in Wireless Sensor Network (TSR) scheme, which works with clustered networks. This approach can effectively reduce the cost of trust evaluation and guarantee a better selection of safest paths that lead to the base station.

Theoretical as well as simulation results show that our scheme requires less communication overheads and consumes less energy as compared to the current typical trust systems for WSNs. Moreover, it detects selfish and defective nodes and prevents us of insider attacks.

Mots-clés

Réputation, Management de confiance, Evaluation de confiance, Energie, Sécurité, Réseau de Capteurs sans fils

Keywords

Reputation, Trust management, Trust evaluation, Energy, Security, Wireless Sensor Network

1. Introduction

Traditional crypto-schemes developed for wired and wireless networks may not prevent sensor networks of malicious attacks. In other words, they may not be suitable for networks with small sensor nodes due to limited bandwidth and stringent node constraints in terms of power and memory. Therefore, it is important to develop trust management schemes and protocols that take into account the intrinsic features of wireless sensor networks. In sensor network security, trust is used as a measure of node's competence in providing required service (Riaz Ahmed Shaikh, *and al.* 2009), (A.A. Pirzada , 2004), (Y.L. Sun *and al.* 2006), (R.A. Shaikh *and al.* , 2006), (M. Momani, and al.2007). It is the level of assurance about a key's authenticity that would be provided by some centralized trusted body to the sensor node (E. Shi and A. Perrig, 2004), (H.S. Ng *and al.* 2006), (Riaz Ahmed Shaikh, *and al.* 2009), (R.A. Shaikh *and al.* 2006). In case of multihop clustering, it helps to select trusted route through which a node can send data to the cluster head. During inter-cluster communication, trust management helps to select trusted route gateway or other trusted cluster heads through which the sender node will forward data to the base station (R.A. Shaikh, *and al.* 2006). In this work we focus on the inter-cluster communication, we give a way to select the safest path that lead to the base station on reducing the cost of trust evaluation. Our proposed scheme focus on the following features:

- TSR does not evaluate trust values of individual nodes. It builds the safest paths by evaluating nodes composed them.
- Our scheme works in a clustered topology.
- Traditional trust management schemes consume a lot of energy during recommendation phase. Our scheme allows recommendations exchange between cluster-heads with applying a light mechanism to reduce communication overheads.
- TSR detects insider attacks, defectives and selfish nodes and eliminates them from network communication.
- It eliminates unsecured paths to guarantee successful communication in a clustered network.

The remainder of the paper is organized as follows: Section 2 presents some related work to trust systems in wireless sensor networks. The proposed trust scheme is described in Section 3. We provide in section 4 a set of tests and evaluate our reputation system with respect to overall network performance; energy consumption and resistance against presence of selfish and malicious nodes. Finally section 5 concludes the paper and suggests some recommendations for further research.

2. Related Work

Recently, some trust management schemes have been proposed such as GMTS (R.A. Shaikh, *and al.* 2006), PLUS (Z. Yao *and al.* 2006)., RFSN (S. Ganeriwal and M.B. Srivastava, 2004), LDTS (Li, X.; *and al.* 2013). Trust-Based Security for Wireless Ad Hoc and Sensor Networks (A. Boukerche, *and al.* 2007), TSRF(A Trust-Aware Secure Routing Framework in Wireless Sensor Networks, Junqi Duan and al.2014), 2-ACKT(Two-Way Acknowledgment-Based Trust Framework for Wireless Sensor Networks, X. Anita, *and al.* 2013), A Secure Trust Establishment Scheme for Wireless Sensor Networks(Farruh Ishmanov, *and al.* 2014). In the following, we describe briefly some of them. In (Z. Yao *and al.* 2006), Z. Yao *and al.* have proposed PLUS protocol for wireless sensors networks. The authors adopt a localized distributed approach. Trust evaluation is based on either direct or indirect observations. S.Ganeriwal *and al.* have proposed RFSN (S.Ganeriwal *and al.* 2008), (S. Ganeriwal and M.B. Srivastava, 2004) scheme for sensor networks, where each sensor node maintains the reputation for neighboring nodes only. Trust values are calculated on the basis of that reputation and they use Bayesian formulation for representing reputation of a node. RFSN assumes that the node has enough interactions with the neighbors so that the reputation can reach a stationary state.

However, if the rate of node mobility is higher, reputation information will not stabilize. In RFSN, no node is allowed to disseminate bad reputation information. If it is assumed that bad reputation is implicitly included by not giving out good reputation, then in that case, the scheme will not be able to cope with uncertain situations (H. Chen *and al.*, 2007).

Shaikh R.A. and. al. have proposed lightweight Group-based Trust Management Scheme (GTMS) (R.A. Shaikh *and al.*, 2006) for wireless sensor networks. Within a cluster, each sensor node calculates individual trust values for all other nodes based on the direct or indirect observations. Based on the trust value, nodes are classified into three categories: 1) trusted, 2) un-trusted or 3) un-certain. In the same way, each cluster maintains the trust value of other clusters (Riaz Ahmed Shaikh *and al.*, 2010).

3. Trust framework for a secured routing in wireless sensor networks

Trust Framework for a Secured Routing in Wireless Sensor Network (TSR) is a light trust scheme that works in a clustered topology and evaluates the paths reliability in a sensor network basing on:

- Sink's acknowledgements.
- Neighbors recommendations.

Our protocol guarantee a secured routing with employing a best path searching technique. The new of this protocol is the global trust measurement for a group of nodes forming a path. In the trust schemes presented until now, if sensor node forwards received packets to the next hop, we qualify it as trusted. Without taking into account what is the end receiver of these packets. In our protocol, if a trusted node has selfish nodes as neighbors, the trustworthiness of path to sink via this node will be reduced. The trusted next hop selection is not sufficient to be sure that the packet will be received by destination. The reliable path construction is the goal of our scheme. Consider as a node "S" send packet to one reliable neighbor "V", if node "V" relays the received packet from "S" to one selfish neighbor "A", the reliability of the path S→V→A will be reduced. So the trust score of "V" will be decremented in the node memory of "S". We assume in the following that the sink has a signal power that can reach the entire network.

For evaluating the trust degree, our scheme requires three phases:

1. Successful interactions calculation
2. Exchange recommandations
3. Aggregation at CH level.

3.1 Successful interactions calculation

Each *CH* (Cluster-head) calculates successful interactions using the acknowledgements received from the sink. Thus, a sequential number *Seq* of 2 bytes is assigned for each data packet created to identify it. Once a *CHi* makes decision about the direct destination (first hop) of packet forwarding, it save its identity IDI (first hop) of 2 bytes. When a *CH* send packet to sink, it send it with its sequential number *Seq*. At the beginning of communication, that one is considered successful. When the sink receives a data packet, it reads its cache and compares the sequential number of current packet with the one of the last packet coming from the same *CHi*. If the current sequential number *Seqi* is not the following of the last one *Seqj* (*i* is not equal to *j*+1), the sink will send the value of *Seqj* to *CHi*. This represents also an acknowledgement of previous packets. Periodically, an acknowledgment is received by all the *CHs* from the sink, even if there is no packet loss. This acknowledgement informs *CHs* of lost packets and knowledge the previous packets. At the reception of an acknowledgement from the sink, in case of packet loss, the *CH* search in its cache the identity of direct destination (IDI) of the lost packet. Once finding, it decrements the number of successful interactions with it. With this manner a sensor node has not need to use promiscuous mode to check if its neighbor's forward packets, so communication overheads is reduced.

3.2 Exchange recommendations

Each round is devised into sub-periods, after each sub-period, CHs broadcast the vector of recommendations of *n**2 bytes that contains the identities of neighbors judged not reliable.

- *n* is the number of nodes judged not reliable.

At the reception of these recommendation vectors, the number of good recommendations is incremented for nodes that do not include within this vector. The process of recommendations exchange is executed periodically, without calling of recommendations requests, and then we conserve considerably node battery. This exchange is less costly compared with others schemes presented in literature. Taking for example the PLUS protocol, for evaluating one neighbor, a pair of packets must be exchanged, a request EReq of 2 bytes for asking a recommendation and a response Erep of 6 bytes for responder to this request.

3.3 Aggregation at *CH* Level

The trust value of a neighbor will be calculated as shown in formula (1):

$$T_{i,j} = \frac{\alpha}{2}\left(\frac{GI_{i,j}}{NI_{i,j}} + \frac{GR_{i,j}}{NR_{i}}\right) \quad (1)$$

When:

- $T_{i,j}$ Trust value of a link *i*→*j*.

- $GI_{i,j}$ The number of successful interactions at the link $i \rightarrow j$.
- $NI_{i,j}$ The number of interactions carried out by the link $i \rightarrow j$.
- $GR_{i,j}$ The number of good recommendations that node i received about the node j.
- NR_i The total number of recommendations received at node i (the number of times a node receives the trust vector).
- α Each node has a value of this coefficient, it equal to 1 when no neighbor declares this node as "attack". For each reception to recommendation "attack", the α coefficient is decremented so as:

$$\alpha = \frac{K_{i,j}}{NbNeighbor_i} \qquad (2)$$

- $K_{i,j}$ is the number $nodei's$ neighbors that do not declare the $node\ j$ as "attack".
- $NbNeighbor_i$ is the total number of $nodei's$ neighbors.
- This division out of 2 because a trust value is considered to be a numerical quantity lying between 0 and 1 (inclusive) as suggested in (Y.L. Sun *and al.*,2006), (G. Theodorakopoulos and J.S. Baras, 2006), and (H. Jameel *and al.* , 2005).

3.4 Representation of Trust levels

One of TSR feature is once the trust values are updated the decision making became a simple process. Each CH separates its neighbors in three groups according to these following demands:

$$\text{Level } (CH_j) = \begin{cases} GOOD & if \quad T_{i,j} \geq \gamma \\ MIDDLE & if \quad \gamma < T_{i,j} < \beta \\ ATTACK & if \quad T_{i,j} < \beta \end{cases}$$

- β is the threshold to judge a neighbor as attack and γ is the value from what a node is judged GOOD.
- With the reception of a message declared one node as attack, α will be decremented, as shown in formula (2).

A selfish node can improve its score and join the group of reliable nodes if its trust degree overtakes the threshold fixed beforehand (β). Else, if its trust degree is less than the threshold, node is considered as attack or defective node and it cannot improve its score. Table.1 shows the different types of TSR packets.

Type	Packet	Size
DataPacket (CM → CH, CH → Sink)	Data (variable), SeqNum (2 bytes), the source (2 bytes)	4 bytes + size of data
RecPacket (CH → CH)	N (number of nodes judged no reliable), ID of node (2 bytes)	2 bytes x N (size of vector)
Ack (Sink → CH)	SeqNum (2 bytes), ID of destination (2 bytes)	4 bytes

Table 1. TSR packets.

4. Tests And Evaluations

For evaluating the performances of our protocol TSR, a comparative study between our protocol TSR and two other ones PLUS and RFSN will be presented in this section using OMNET ++ simulator. For energy consumption analysis, we assume first order radio model that is widely used by the researchers as in (H. sook Kim and K. jun Han, 2005) and (Y. Massad *and al.*, 2008), in which the energy expanded to transfer a k-bit packet to a distance d and to receive that packet, as suggested by H.O. Tan and I. Korpeoglu in (H. O. Tan and I. Korpeoglu, 2003) is:

$$ETx(k,d)=k^*Eelec+k^*d2\ ^*Eamp \qquad (3)$$
$$ERx(k)=k^*Eelec$$

Here, *Eelec* is the energy dissipation of the radio in order to run the transmitter and receiver circuitry and is equal to 50*nJ/bit*. The *Eamp* is the transmit amplifier that is equal to 100*pJ/bit/m*^{2}. The *Eelec* and *Eamp* are the device specific parameters. The values that we use here for the theoretical analysis are the assumed values, which are commonly used in the literature (H. sook Kim and K. jun Han, 2005), (Y. Massad *and al.* 2008).

Scenario 1: Recommendations between cluster-heads

In the case of PLUS and RFSN, when a sensor node has need a recommendation about other nodes, it send a request to its neighbors. In the case of our scheme TSR, a CH receives periodically from its neighbors a recommendation vector that specifies the selfish nodes. The request for asking recommendation does not exist in our scheme. In the case of TSR the consumed energy by the transmitter of recommendation packet is:

$$E = ETx\ (16{*}\mathrm{m},\ \mathrm{d}) \tag{4}$$

The consumed energy by the receiver of recommendation packet:

$$E = ERx\ (16{*}m)\ \mathrm{x}\ Nb \tag{5}$$

- *m* is the size of recommendation vector.
- *Nb* represents the number of neighbors.
- 16 represents the size of field reserved to node identity.

In the case of RFSN, the consumed energy by the transmitter of recommendation packet is:

$$E = n \times [ETx\ (16,\ d) + ERx\ (48)] \tag{6}$$

When:

- *n* represents the number of trusted nodes into a cluster.
- 16 and 48 present respectively the size of request packet and the size of recommendation packet of RFSN scheme.

Also, in RFSN the consumed energy by the transmitter of response packet is:

$$\begin{gathered} E = ETx\ (48,\ d) + ERx\ (16) \\ E = 16\ {*}Eelec{+}\ 48\ (Eelec{+}\ d2\ {*}Eamp) \end{gathered} \tag{7}$$

In case of PLUS protocol, the consumed energy by the transmitter of recommendation packet is:

$$\begin{gathered} E = ETx\ (16,\ d) + (n{-}2)ERx\ (48) \\ E = 16(Eelec{+}\ d2Eamp) + (48\ Eelec) \end{gathered} \tag{8}$$

When:

- *n* is the number of cluster-heads.

For consumed energy by the transmitter of response packet is:

$$E = ETx\ (48,\ d) + ERx\ (16)\ \mathrm{E} = 48(Eelec{+}\ d2{*}Eamp) + (16\ Eelec) \tag{9}$$

- 16 and 48 present respectively the size on bits of request and response packet of PLUS scheme.

The summary of energy consumption during recommendations between cluster-heads is presented in table 2. When: *n* is the total number of neighbors in PLUS and RFSN and *m* is the size of recommendation vector in TSR protocol.

	TSR	RFSN	PLUS
Number of sanded packets	0	t≤n−2 For evaluating a one neighbor	1 For evaluating a one neighbor
Number of recommandations received	1 For evaluating all neighbors	t≤n−2 For evaluating a one neighbor	n-2 For evaluating a one neighbor
Size of request	/	16 bits	16 bits
Size of response	m*16 bits	48 bits	48 bits
The consumed energy on request	E_{Tx} (m*16, d)	n x [E_{Tx} (16, d) + [E_{Rx} (48)]	E_{Tx} (16, d) + (n – 2) E_{Rx} (48)
The consumed energy on response	E_{Rx} (m*16)	E_{Tx} (48, d) + E_{Rx} (16)	E_{Tx} (48, d) + E_{Rx} (16)

Table 2. Pairs recommendations between cluster-heads.

In order to compare energy consumption during recommendation scenarios between cluster-heads. We assume to have the following simulation parameters:

Parameter	Value
Surface	**100*100*50**
Localization of base station	**(0,0,0)**
Number of nodes	**100, 200, 300**
Number of base stations	**1**
Period of Round	**10 s**
Simulation Time	**200 s**
Number of selfish CHs	**3, 5, 7**

Table 3. Simulation parameters of scenario 1.

The figure 1 shows clearly that TSR consumes less energy compared with RFSN and PLUS schemes. In TSR protocol, nodes do not send requests for asking recommendations from their neighbors. The sending of recommendation packets is carried out periodically. While, in RFSN and PLUS, cluster-heads send recommendation requests every time a CH has need recommendation about one neighbor. This figure shows also that the PLUS scheme consumes less energy than RFSN, because that in PLUS scheme the request packet is broadcasted of all its neighbors, when needed recommendation. While, in the RFSN protocol, the request packet is sanded on unicast to all its trusted neighbors.

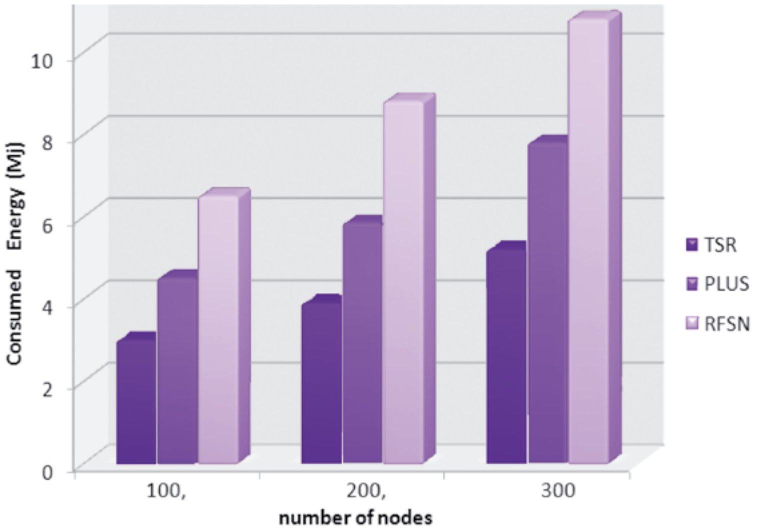

Figure 1. Consumed energy in each scheme TSR, RFSN and PLUS for recommendations scenarios.

Scenario 2: Loss packet rate in the presence of selfish nodes

In a scenario of 100 nodes, using these parameters we are shown the following results:

Parameter	Value
Surface	**100*100*50**
Localization of base station	**(0,0,0)**
Number of nodes	**100**
Number of clusters	**8**
Number of base stations	**1**
Period of Round	**10 s**
Simulation Time	**200 s**
Maximum rate of selfish CHs	**37,5**

Table 4.Simulation parameters of scenario 2

Figure 2 compares the packet loss rate with applying the TSR protocol, and without applying it. Values of γ and β are fixed after several simulations at respectively 0,50 and 0,23.

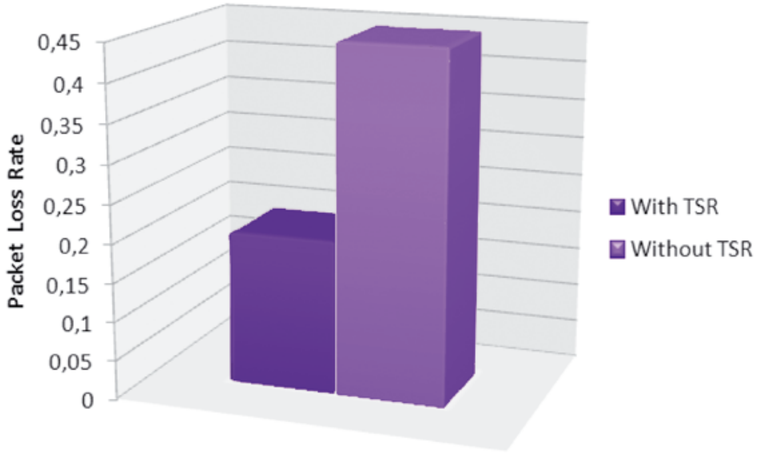

Figure 2. The packet loss rate with TSR and without TSR.

Results presented in this figure are obtained, for a network size of 100 nodes. The trust degree attributed to nodes reduces interactions with selfish nodes, so we reduce considerably the packet loss rate.

Scenario 3: Packet loss rate in the presence of 37, 5% of selfish nodes and of 12, 5 % of Black Hole attacks

In a network of 100 nodes, we show the following results. Simulations have shown an important packet loss rate during the first rounds in the case of application of TSR scheme. That can be explained, with considering all neighbors as trusted at deployment. By disobeying to forward packets, communication with selfish nodes weakens. This reduces in parallel the packet loss rate. The figure 3 presents the number of packet lost in the presence of Black Hole attacks and selfish nodes in a network of 9 clusters.

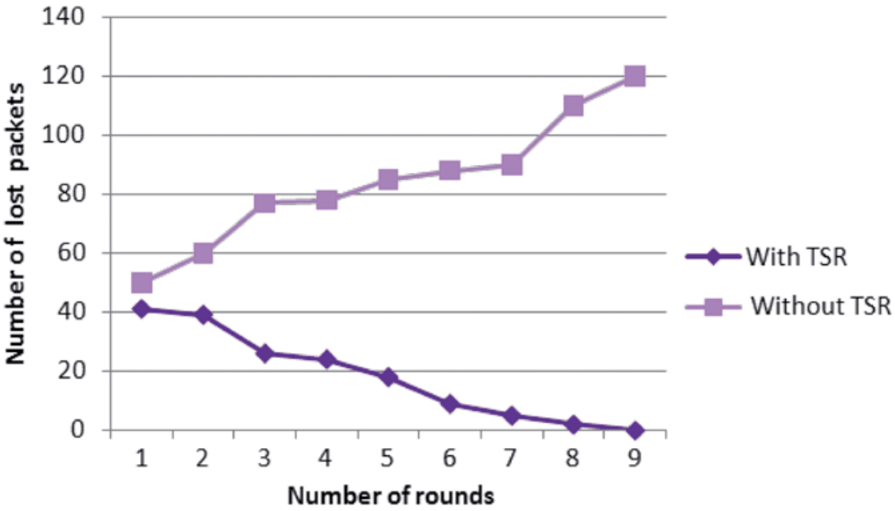

Figure 3. Number of lost packets with 12,5 % of attacks and 37,5% of selfish nodes.

5. Conclusion

In this paper, we have proposed a light scheme that can cope with insider attacks in WSNs. TSR allows carrying out successful interactions in sensor networks, with its relevant technique that focus on safest path searching. TSR minimizes the energy consumption in the recommendations exchange phase. Although, the choice of the best path ensure that the destination will receive packets, but these packets can suffer from falsification. So, the challenging problem is to ensure that the data does not been modified. This motivates future work.

6. References

A.A. Pirzada and C. McDonald. (2004). *Establishing Trust in Pure Ad-Hoc Networks.* Proc. 27th Australasian Computer Science Conf. (ACSC '04), pp. 47-54, Jan. 2004.

A. Boukerche, X. Li, *and al.*(2007). *Trust-Based Security for Wireless Ad Hoc and Sensor Networks.* Computer Comm., vol. 30,pp. 2413-2427, Sept. 2007.

A. Perrig, R. Szewczyk, *and al.*(2002). *SPINS: Security Protocols for Sensor Networks*. Wireless Networks Journal (WINET), 8(5):521–534, September 2002.

E. Shi and A. Perrig. (2004). *Designing Secure Sensor Networks*. IEEE Wireless Comm., vol. 11, no. 6, pp. 38-43, 2004.

Farruh Ishmanov, Sung Won Kim *and al.* (2014). *A Secure Trust Establishment Scheme for Wireless Sensor Networks*. Sensors 2014, 14, 1877-1897; doi:10.3390/s140101877.

G. Theodorakopoulos and J.S. Baras.(2006). *On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks*. IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 318-328, Feb. 2006.

H. Chen, H. Wu, *and al.*(2007). *Reputation-Based Trust in Wireless Sensor Networks*. Proc. Int'l Conf. Multimedia and Ubiquitous Eng. (MUE '07), pp. 603-607, Apr. 2007.

H. Jameel, L.X. Hung, *and al.*(2005). *A Trust Model for Ubiquitous Systems Based on Vectors of Trust Values*.Proc. Third IEEE Int'l Security in Storage Workshop (SISW '05), pp. 674-679, Dec. 2005.

H. sook Kim and K. jun Han. (2005). *A power efficient routing protocol based on balanced tree in wireless sensor networks.* in Proc. of the 1st Int. Conference on Distributed Frameworks for Multimedia Applications (DFMA '05), Feb. 2005, pp. 138–143.

H.S. Ng, M.L. Sim, *and al.*(2006). *Security Issues of Wireless Sensor Networks in Healthcare Applications*. BT Technology J., vol. 24, no. 2, pp. 138-144, Apr. 2006.

H. O. Tan and I. Korpeoglu.(2003). *Power efficient data gathering and aggregation in wireless sensor networks*.ACM SIGMOD Record, vol. 32, no. 4, pp. 66–71, Dec. 2003.

Junqi Duan, Dong Yang, *and al.* (2014). *TSRF: A Trust-Aware Secure Routing Framework in Wireless Sensor Networks*. International Journal of Distributed Sensor Networks Volume 2014 , Article ID 209436, 14 pages.

Li, X.; Zhou, F, *and al.*(2013). *LDTS: A Lightweight and Dependable Trust System for Clustered Wireless Sensor Networks*. IEEE Trans. Inf. Forensics Security 2013, 8, 924–935.

M. Momani, S. Challa, *and al.*(2007). *Modelling Trust in Wireless Sensor Networks from the Sensor Reliability Prospective*. Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecomm., T.S. *et al.*, ed., pp. 317-321, Springer, 2007.

R.A. Shaikh, H. Jameel, *and al.*(2006). *Trust Management Problem in Distributed Wireless Sensor Networks*.Proc. 12th IEEE Int'l Conf. Embedded Real-Time Computing Systems and Applications (RTCSA '06), pp. 411-414, Aug. 2006.

Riaz Ahmed Shaikh, Hassan Jameel, *and al.*(2009). *Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks*. IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 20, NO. 11, NOVEMBER 2009.

Riaz Ahmed Shaikh, Young-Koo Lee, *and al.*(2010). *An Extended Energy Consumption Analysis of Reputation-based Trust Management Schemes of Wireless Sensor Networks.* JOURNAL OF NETWORKS, VOL. 5, NO. 3, MARCH 2010.

S. Ganeriwal and M.B. Srivastava. (2004). *Reputation-Based Framework for High Integrity Sensor Networks.* Proc. ACM Workshop Security of Ad Hoc and Sensor Networks (SASN '04), pp. 66-67, Oct. 2004.

S. Ganeriwal, L. K. Balzano, *and al.* (2008). *Reputation-based framework for high integrity sensor networks.* ACM Trans. Sen. Netw., vol. 4, no. 3, pp. 1–37, 2008.

X. Anita, J. Martin Leo Manickam, *and al.*(2013). *Two-Way Acknowledgment-Based Trust Framework for Wireless Sensor Networks.* International Journal of Distributed Sensor Networks Volume 2013, Article ID 952905, 14 pages, 4 April 2013.

Y.L. Sun, W. Yu *and al.*(2006). *Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks.* IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 305-317, Feb. 2006.

Y. Massad, M. Goyeneche, *and al.* (2008). *Data aggregation in wireless sensor networks.* in Proc. of the 3rd Int. Conference on Information and Communication Technologies: From Theory to Applications (ICTTA 2008), April 2008, pp. 1–6.

Z. Yao, D. Kim, *and al.*(2006). *PLUS: Parameterized and localized trust management scheme for sensor networks security.* in Proc. of the 3rd IEEE Int. Conf. on Mobile Adhoc and Sensor Systems, Vancouver, Canada, Oct. 2006, pp. 437–446.