Journal of Networks, Vol 5, No 3 (2010)

Journal of Networks, Vol 5, No 3 (2010), 283-291, Mar 2010
doi:10.4304/jnw.5.3.283-291

An Extended Energy Consumption Analysis of Reputation-based Trust Management Schemes of Wireless Sensor Networks

Riaz Ahmed Shaikh, Young-Koo Lee, Sungyoung Lee

Abstract

Energy consumption is one of the most important parameters for evaluation of a scheme proposed for wireless sensor networks (WSNs) because of their resource constraint nature. Comprehensive comparative analysis of proposed reputation-based trust management schemes of WSNs from this perspective is currently not available in the literature. In this paper, we have presented a theoretical and simulation based energy consumption analysis and evaluation of three state-of-the-art reputation-based trust management schemes of WSNs. Results show that the GTMS scheme consume less energy as compared with the RFSN and PLUS schemes.

Keywords

Reputation; Sensor networks; Trust management;Trust evaluation

Full Text: PDF

Journal of Networks (JNW, ISSN 1796-2056)

An Extended Energy Consumption Analysis of Reputation-based Trust Management Schemes of Wireless Sensor Networks

Riaz Ahmed Shaikh, Young-Koo Lee, Sungyoung Lee
Dept. of Comp. Eng., Kyung Hee University, Global Campus, Korea
riaz@oslab.khu.ac.kr, yklee@khu.ac.kr, sylee@oslab.khu.ac.kr

***Abstract*— Energy consumption is one of the most important parameters for evaluation of a scheme proposed for wireless sensor networks (WSNs) because of their resource constraint nature. Comprehensive comparative analysis of proposed reputation-based trust management schemes of WSNs from this perspective is currently not available in the literature. In this paper, we have presented a theoretical and simulation-based energy consumption analysis and evaluation of three state-of-the-art reputation-based trust management schemes of WSNs. Results show that the GTMS scheme consume less energy as compared with the RFSN and PLUS schemes.**

***Index Terms*— Reputation, Sensor networks, Trust management, Trust evaluation**

I. INTRODUCTION

Trust in general is the level of confidence in a person or a thing. More precisely trust can be defined as: "the quantified belief by a trustor with respect to the competence, honesty, security and dependability of a trustee within a specified context" [1]. Reputation is a notion sometimes confused with trust; it is defined as "the global perception about the entity's behavior norms based on the trust that other entities hold in the entity" [2]. Reputation-based trust management schemes are used in various diverse domains, such as, e-commerce systems [3], ad-hoc networks [4]–[6], and peer-to-peer networks [7]–[9]. In this paper, we will discuss them from the perspective of wireless sensor networks (WSNs).

Reputation-based trust management schemes are useful in many application scenarios [10]. For example, they provide aid to the routing protocols for making reliable routing decisions [11], such as, next hop should not be malicious or faulty one. Also, these schemes provide assurance during various security enforcement phases (authentication, key management etc.) that all communicating nodes are trusted. Additionally, these schemes are helpful in providing corresponding access control based on judging the quality of sensor nodes and their services [12].

Wireless sensor networks comprises of resource constraint devices having limited memory, energy and computation power. Many reputation-based trust management schemes [2], [10], [13], [14] have been proposed for WSNs. However, comprehensive comparative analysis from energy consumption perspective is currently not available in the literature. This is important to analyze and evaluate due to resource constraint nature of WSNs. Therefore, in this paper, we have tried to fill this gap by presenting theoretical and simulation-based energy consumption analysis and evaluation of three state-of-the-art reputation-based trust management schemes: 1) RFSN [2], 2) PLUS [14], and 3) GTMS [10]. We have performed comparison in different scenarios and results show that the GTMS scheme consumed less energy as compared with the RFSN and PLUS schemes.

The rest of the paper is organized as follows: Section 2 contains description of proposed trust management schemes. Sections 3 and 4 presents theoretical and simulation-based energy consumption analysis and evaluation respectively. Section 5 concludes the paper.

II. DESCRIPTION OF PROTOCOLS

A. RFSN Protocol

S. Ganeriwal and M. B. Srivastava [2], [15] have proposed Reputation-based Framework for Sensor Networks (RFSN), where each sensor node maintains the reputation for neighboring nodes. On the basis of that reputation trust values are calculated. Based on the trust value nodes are classified into two categorized: cooperative (trusted) and not cooperative (un-trusted).

Whenever a node needs recommendation value of the other node it will send a request packet (Req) to trusted nodes of the neighborhood. This request packet contain

Manuscript received March 31, 2009; revised July 18, 2009; accepted September 10, 2009.

This paper is an extended version of our paper entitled "Energy Consumption Analysis of Reputation-based Trust Management Schemes of Wireless Sensor Networks", which appeared in the Proceedings of the 3rd International Conference on Ubiquitous Information Management and Communication, Suwon, Korea, Jan 2009, pp 652-656. © 2009 ACM.

Corresponding Author: Sungyoung Lee.

This research was supported by the MKE (Ministry of Knowledge Economy), Korea, under the ITRC (Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Advancement) (IITA-2009-(C1090-0902-0002)) and was supported by the IT R&D program of MKE/KEIT [10032105, Development of Realistic Multiverse Game Engine Technology]. This work also was supported by the Brain Korea 21 projects and Korea Science & Engineering Foundation (KOSEF) grant funded by the Korea government (MOST) (No. 2008-1342).

doi:10.4304/jnw.5.3.283-291

the identity of the evaluating node. In response to the Req packet, trusted neighborhood nodes send back reply messages (Rep) to the requester. This reply packet contain the identity of the evaluating node and its trust value. Packet description of the RFSN scheme is shown in Table I.

TABLE I.
PACKETS OF RFSN SCHEME

Type	Payload	Size of payload
Req	ID of evaluating node (2 bytes)	2 bytes
Rep	ID of evaluating node(2 bytes), trust value(4 bytes)	6 bytes

B. PLUS Protocol

Z. Yao et al. [14] have proposed Parameterized and Localized trUst management Scheme (PLUS) for WSNs. The authors adopt a localized distributed approach and trust is calculated based on either direct observations or indirect observations. Based on the trust value nodes are classified into four categories: 1) Distrust (untrustworthy), 2) Minimal (low trust), 3) Average (common trustworthy), and 4) Good (trustworthy).

Whenever a node needs recommendation about another node, it will broadcast a request packet ($EReq$) to its neighbors. This packet contain the identity of the evaluating node. In response all the nodes (except the node whose is going to be evaluated) send back a response packet ($ERep$) to the requester. Once all the response packets are received, the requester will calculate the final trust value. If the node find any misbehavior about the evaluated node, then the node will broadcast a exchange information packet ($EInf$) to its neighbors. This packet contain information about identity of the node and error code. Based on the trust policy, the neighboring nodes sends out its opinion: exchangeAck ($EAck$) packet in case if they agree with the sender, otherwise neighbors will reply with exchageArgue ($EArg$) packet. Packet description of the PLUS scheme is shown in Table II.

TABLE II.
PACKETS OF PLUS SCHEME

Type	Payload	Size of payload
EReq	ID of evaluating node (2 bytes)	2 bytes
ERep	ID of evaluating node(2 bytes), trust value(4 bytes)	6 bytes
EInf	ID of evaluating node(2 bytes), Error code(2 bytes)	4 bytes
EAck	ID of evaluating node (2 bytes)	2 bytes
EArg	ID of evaluating node (2 bytes), trust value(4 bytes)	6 bytes

C. GTMS Protocol

Shaikh R.A. et. al. [10] have proposed lightweight Group-based Trust Management Scheme (GTMS) for wireless sensor networks. With in 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 maintain the trust value of other clusters.

The GTMS scheme is comprises of four pairs of request and response packets as shown in Table III.

Pair 1: used for Peer Recommendation. Whenever a node x needs recommendation from node y about z, it sends a request packet (iTReq) of size 2 bytes to node y. In response, node y send a response packet (iTRep) of size 3 bytes to node x. The iTRep contains the trust value of z.

Pair 2: used for the transfer of trust vector from node to cluster head (CH). After a periodic interval, the CH j broadcast a request (iVReq) packet inside the group. In response all nodes that belongs the cluster j send back a response packet (iVRep) of size $1 + 2.25v$ bytes, where $v \leq n - 1$ represents the length of the trust vector and n represents the total number of nodes in the cluster or group.

Pair 3: used for getting recommendation from base station (BS) by CH. Whenever a CH j need a recommendation from the BS about another cluster k, it send a request packet (oTReq) to the BS. In response, the BS send a response packet (oTRep) to the CH j that contain the trust value of CH k. The size of the response packet is 3 bytes.

Pair 4: used for the transfer of trust vectors from CH to BS. After every periodic interval of time, the base station multicast a request packet (oVReq) to all CHs in the network. In response, all CHs send back a response packet (oVRep) of size $1 + 3v$ bytes, where $v \leq |G|$ represents the length of the trust vector and $|G|$ represents the total number of clusters or groups.

III. THEORETICAL ANALYSIS AND EVALUATION

For the energy consumption analysis, we assume first order radio model as defined in [16] that is widely used by the researchers as in [17]–[20]. However, other energy models could also be used, such as [21], [22]. In first order radio model, 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 [16] is:

$$\begin{array}{l} E_{Tx}(k,d) = kE_{elec} + kd^2E_{amp} \\ E_{Rx}(k) = kE_{elec} \end{array} \tag{1}$$

Here, E_{elec} is the energy dissipation of the radio in order to run the transmitter and receiver circuitry and is equal to $50nJ/bit$. The E_{amp} is the transmit amplifier that is equal to $100pJ/bit/m^2$. The E_{elec} and E_{amp} are the device specific parameters. The values that we used here for the theoretical analysis are the assumed values, which are commonly used in the literature [17]–[20].

TABLE III.
PACKETS OF GTMS SCHEME

		Type	Payload	Size (payload)
packets move inside cluster	Pair 1: for peer recommendation	iTReq (SN-SN)	ID of evaluating node (2 bytes)	2 bytes
		iTRep (SN-SN)	ID of evaluating node (2 bytes), trust value (1 byte)	3 bytes
	Pair 2: for transfer of trust vector	iVReq (CH-SN)	Nil	-
		iVRep (SN-CH)	Vector length v(1 byte), ID (2 bytes) and trust state (1 bit) of v member nodes	1+2.25v bytes
packets move outside cluster	Pair 3: for peer recommendation	oTReq (CH-BS)	ID of evaluating node (2 bytes)	2
		oTRep (BS-CH)	ID of evaluating node (2 bytes), trust value (1 byte)	3 bytes
	Pair 4: for transfer of trust vector	oVReq (BS-CH)	Nil	-
		oVRep (CH-BS)	Vector length v(1 byte), ID (2 bytes) and trust value (1 byte) of other clusters	1+3v bytes

We have performed theoretical energy consumption analysis at the higher level. For the fair comparison, we assumed that routing and MAC protocols are same. For theoretical energy consumption analysis and evaluation, we must have the information about the number of bits transmitted and received during trust evaluation phase between different nodes. The size of packet is mainly dependent on the size of payload. Header and tailer fields of a packet generally remain constant. Therefore we have ignored those during theoretical analysis given below. We have performed the theoretical energy consumption analyses and evaluation of various trust management schemes in four different scenarios.

A. Scenario 1: Peer recommendation between member nodes

Within a cluster, peer recommendation take place when nodes do not have any prior direct interaction experience with other node. Based on the peer recommendation trust value of node is calculated. For example, in case of multihop routing, it helps to select trusted en-route nodes through which a node can send data to the cluster head. Also, it helps new elected cluster head to get recommendation about the gateway nodes from other member nodes in case if it has no prior direct interaction experience.

When a sensor node needs a recommendation about other nodes, it will send a request packet to its peers. In the case of the GTMS scheme, the requester will send request to all the the nodes except the un-trustful ones. Assume that out of n nodes, j nodes are trusted and uncertain. Then, the total energy consumed at the requester end is,

$$E = j\left[E_{Tx}(k, d) + E_{Rx}(k')\right] \tag{2}$$

where, $0 < j \le n-2$, and n is the number of nodes in the group. For peer recommendation, the payload size of a request packet is 2 bytes, thus $k = 16$ bits. The payload size of a response packet is 3 bytes, thus $k' = 24$ bits. So the total energy consumed at the requester end is:

$$\begin{aligned} E &= j\left[E_{Tx}(16, d) + E_{Rx}(24)\right] \\ E &= j\left[16(E_{elec} + d^2 E_{amp}) + (24 E_{elec})\right] \end{aligned} \tag{3}$$

Also for the GTMS, the energy consumed at the responder end is:

$$\begin{aligned} E &= E_{Rx}(16) + E_{Tx}(24, d) \\ E &= 16E_{elec} + 24(E_{elec} + d^2 E_{amp}) \end{aligned} \tag{4}$$

Energy consumption during peer recommendation of other schemes is shown in Table IV. In the case of the RFSN scheme, the energy consumption at the requester end is:

$$E = t \times \left[E_{Tx}(16, d) + E_{Rx}(48)\right] \tag{5}$$

where t represents the number of trusted node in the cluster ($0 < t \le n-2$), 16 and 48 represents the size of the request and response packets of RFSN scheme respectively. Also for the RFSN, the energy consumed at the responder end is:

$$\begin{aligned} E &= E_{Rx}(16) + E_{Tx}(48, d) \\ E &= 16E_{elec} + 48(E_{elec} + d^2 E_{amp}) \end{aligned} \tag{6}$$

In the case of the PLUS scheme, the minimum energy consumption at the requester end is:

$$\begin{aligned} E &= E_{Tx}(16, d) + (n-2)E_{Rx}(48) \\ E &= 16(E_{elec} + d^2 E_{amp}) + (n-2)(48 E_{elec}) \end{aligned} \tag{7}$$

Here 16 and 48 represents the size of the request and response packets of the PLUS scheme respectively. Also for the PLUS, the energy consumed at the responder end is:

$$\begin{aligned} E &= E_{Rx}(16) + E_{Tx}(48, d) \\ E &= 16E_{elec} + 48(E_{elec} + d^2 E_{amp}) \end{aligned} \tag{8}$$

In order to compare the energy consumption during peer recommendation scenario within the a cluster, we have assumed that a single group consists of nine nodes arranged in a grid fashion as shown in Figure 1. For this small topology, we have taken two scenarios. In the first scenario we have only two requesters getting recommendation from one available trusted node, and in second scenario, two requesters are getting recommendation from

TABLE IV.
PEER RECOMMENDATION OF SENSOR NODES WITHIN A CLUSTER

	GTMS	RFSN	PLUS
Number of request packets forwarded	$j \leq n-2$	$t \leq n-2$	1
Number of response packets received	$j \leq n-2$	$t \leq n-2$	$n-2$
Size of request packet (payload only)	16 bits	16 bits	16 bits
Size of response packet (payload only)	24 bits	48 bits	48 bits
Energy consumption at requester	$j[E_{T_x}(16,d)+E_{R_x}(24)]$	$t[E_{T_x}(16,d)+E_{R_x}(48)]$	$E_{T_x}(16,d)+(n-2)\times E_{R_x}(48)$
Energy consumption at responder	$E_{T_x}(24,d)+E_{R_x}(16)$	$E_{T_x}(48,d)+E_{R_x}(16)$	$E_{T_x}(48,d)+E_{R_x}(16)$

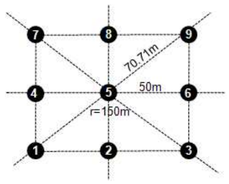
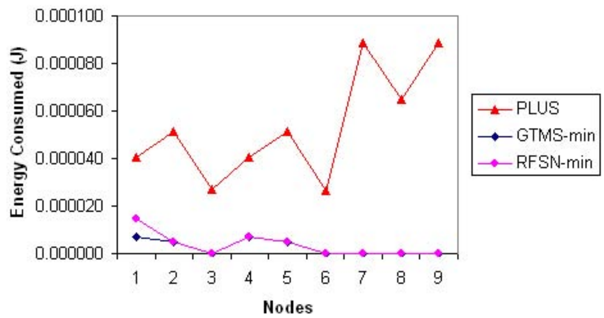


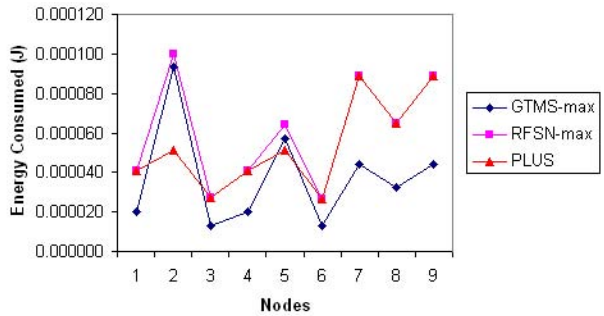
Figure 1. Sample Group Scenario

all the available trusted nodes (excluding the one who is going to be evaluated) by the requester. First scenario shows the minimum energy consumption analysis and second scenario shows the maximum energy consumption analysis of the group.

Figure 2(a) shows the minimum energy consumption analysis (first scenario), which shows that GTMS consume less energy as compared to the PLUS scheme. Also, GTMS consume approximately same amount of energy as RFSN scheme. Figure 2(b) illustrates the maximum energy consumption analysis (second scenario), which shows that the GTMS scheme overall consume less energy in a group then the PLUS scheme at the cost of slightly more energy consumption at the requester ends. Also, as compared to the RFSN scheme, GTMS scheme consume less energy at the responder (recommender) ends and approximately same energy at the requester ends.



(a) Minimum energy consumption with 2 requesters (2 need recom. about 3 from 1, and 5 needs recom. about 6 from 4)



(b) Maximum energy consumption with 2 requesters (2 need recom. about 3, & 5 need recom. about 6 from all other nodes)

Figure 2. Energy consumption during peer recommendation scenario of sensor nodes

B. Scenario 2: Peer recommendation between cluster heads

Like members nodes, peer recommendation take place when cluster heads do not have prior direct interaction experience with other cluster heads. For example, cluster heads may communicate with the base station via gateway nodes or other cluster heads. In this case, peer recommendation is useful to select trusted next hop node.

In case of the GTMS scheme, when ever a cluster head need a recommendation value about another group then the cluster head will send a request packet to the base station, in response base station will send back trust value of other group. Therefore, tin case of the GTMS scheme, the total energy consumed at the cluster head will be;

$$\begin{aligned} E &= E_{Tx}(16,d) + E_{Rx}(24) \\ E &= 16(E_{elec} + E_{amp} \times d^2) + 24E_{elec} \end{aligned} \tag{9}$$

where 16 bits represents the size of the request packet and 24 bits represents the size of the response packet. In this case responder is base station which usually does not have any resource constraints. Therefore, we can ignore the energy consumption analysis at the base station.

In case of the RFSN scheme, when ever a cluster head need a recommendation value about another group then the cluster head will send a request packets to its neighboring cluster heads. In response neighboring cluster heads will send back trust value of other group. Therefore, in case of the RFSN scheme, the total energy consumed at the requester cluster head will be;

$$\begin{aligned} &E = \sum_{j=0}^{r} E_{Tx}(16,d) + \sum_{j=0}^{q} E_{Rx}(48) \\ &E = \sum_{j=0}^{r} (16(E_{elec} + E_{amp} \times d^2)) + \sum_{j=0}^{q} (48E_{elec}) \\ &where, q \leq r; \end{aligned} \tag{10}$$

where r represents the number of request packets and q represents the number of response packets. The size of request packet is 16 bits and the size of response packet is 48 bits. The total energy consumed at the responder cluster head will be:

$$E = 16E_{elec} + 48(E_{elec} + E_{amp} \times d^2) \quad (11)$$

In case of the PLUS scheme, when ever a cluster head need a recommendation value about another group then the cluster head will broadcast request packet to its neighboring cluster heads. In response, all neighboring cluster heads will send back trust value of the required group. Therefore, in case of the RFSN scheme, the total energy consumed at the requester cluster head will be;

$$\begin{aligned} E &= E_{Tx}(16, d) + \sum_{j=0}^{q} E_{Rx}(48) \\ E &= 16(E_{elec} + E_{amp} \times d^2) + \sum_{j=0}^{q} (48E_{elec}) \end{aligned} \quad (12)$$

where q represents the number of response packets. The size of request packet is 16 bits and the size of response packet is 48 bits. The total energy consumed at the responder cluster head will be:

$$E = 16E_{elec} + 48(E_{elec} + E_{amp} \times d^2) \quad (13)$$

Summary of energy consumption during peer recommendation of cluster heads is shown in Table V. Here m represents the total number of neighboring cluster heads. In order to compare the energy consumption during peer recommendation scenario between clusters, we have assumed 5 clusters and one base station in the network as shown in Figure 3. In this scenario CH_1 needs recommendation about CH_2 and CH_3 needs recommendation about CH_4.

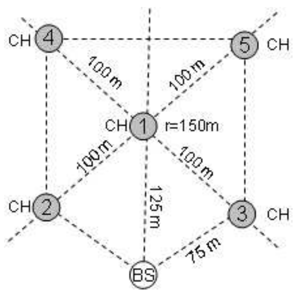


Figure 3. Cluster scenario

Figure 4 clearly shows that the GTMS consumes less energy as compared with the RFSN and PLUS schemes. This is because, in GTMS cluster head only need recommendation from the base station. Whereas, in RFSN and PLUS schemes cluster head need recommendation from its neighboring cluster heads. This figure also illustrates that at the requester ends (CH_1 and CH_3) PLUS scheme consume less energy, because request packet is broadcast to all its neighboring cluster heads. Whereas, in case of the RFSN scheme, the request packet is unicasted to all trusted neighboring cluster heads.

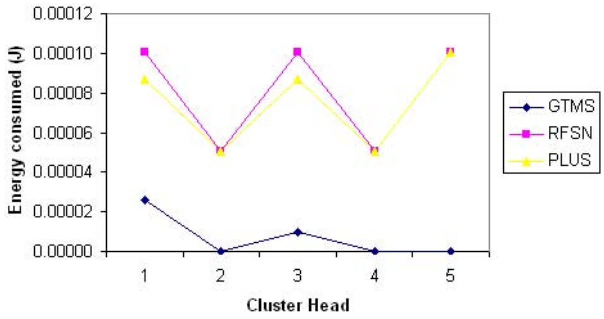


Figure 4. Peer recommendation for cluster heads: 1 needs recommendation for 2 and 3 needs recommendations for 4.

Scenario 3 and 4 are only applicable to the GTMS scheme. Therefore, we have compared the GTMS scheme with the generic Distributed Trust Management Scheme (DTMS) in which each node maintains a one-to-one trust relationship with each other.

C. Scenario 3: Global trust value of each node

In order to calculate the global trust state (e.g. trusted, uncertain or un-trusted) of each member node, cluster head periodically broadcast a request message. In response all member nodes send back a trust state of other nodes to the cluster head. This approach, help cluster head to detect the presence of any malicious node in the group.

Whenever a sensor node gets request to send trust vector from the cluster head, it will send $n-1$ bytes of trust vector data to the cluster head. Here n is the number of nodes in the cluster. At the requester end, the total energy consumed during this phase is the sum of the energy consumed during sending of the request packet (E_{T_x}) plus energy consumed during receiving of the response packet (E_{R_x}) from all member nodes, as given below:

$$E = E_{T_x}(k, d) + \sum_{j=0}^{r} E_{R_x}(k') \quad (14)$$

$$E = k \times (E_{elec} + E_{amp} \times d^2) + \sum_{j=0}^{r} E_{elec} \times k' \quad (15)$$

Here k is the length of the request packet, k' is the length of the response packet and r represents the number of responses received by the requester. Payload of the request packet does not contains any additional information and can be identified by the *type* field present in the header of the packet. As we have already mentioned in earlier discussion that the size of header remains constant for all protocols. Therefore, we can assume that size of the request packet is 1 and, the size of the response packet (k') is $8 + 18v$ bits [See Table III]. Then the total energy consumed at the requester end will be;

$$E = 1 \times (E_{elec} + E_{amp} \times d^2) \ + \sum_{j=0}^{r} E_{elec} \times (8 + 18v) \quad (16)$$

TABLE V.
PEER RECOMMENDATION OF CLUSTER HEADS

	GTMS	RFSN	PLUS
Number of request packets forwarded	1	$r \leq m-1$	1
Number of response packets received	1	$q \leq r$	$q \leq m-1$
Size of request packet (payload only)	16 bits	16 bits	16 bits
Size of response packet (payload only)	24 bits	48 bits	48 bits
Energy consumption at requester	$E_{T_x}(16,d) + E_{R_x}(24)$	$\sum_{j=0}^{r} E_{T_x}(16,d) + \sum_{j=0}^{q} E_{R_x}(48)$	$E_{T_x}(16,d) + \sum_{j=0}^{q} E_{R_x}(48)$
Energy consumption at responder	-	$E_{T_x}(48,d) + E_{R_x}(16)$	$E_{T_x}(48,d) + E_{R_x}(16)$

In the case of the GTMS, $r \leq n-1$ and $v \leq n-1$, where n is the number of nodes in the group, where as in the case of the DTMS $r \leq N-1$ and $v \leq N-1$, where N is the number of nodes in the network.

At the responder end, the total energy consumed during this phase is the sum of energy consumed during receiving of the request packet (E_{R_x}) plus energy consumed during transfer of the response packet (E_{T_x}) as given below:

$$E = E_{elec} \times k + k' \times (E_{elec} + E_{amp} \times d^2) \quad (17)$$

Then the total energy consumed at the responder end will be;

$$E = E_{elec} \times 1 + (8 + 18v) \times (E_{elec} + E_{amp} \times d^2) \quad (18)$$

In the case of the GTMS, $v \leq n-1$ where n is the number of nodes in the group and in the case of the DTMS, $v \leq N-1$, where N is the number of nodes in the network.

Comparison of energy consumption from the requester and responder point of view is shown in Figure 5. In a simulation, the requester and responder reside at the distance of 150 meters from each other. Initially for 100 nodes in the sensor network, we assumed only one cluster. In this case, energy consumption of the GTMS and DTMS at the requester and responder ends remains same. But as we increase the number of clusters in the network, the GTMS shows lower energy consumption as compared with the DTMS. For example, for the case of five clusters in the network comprises of 100 nodes, at the requester end, the GTMS scheme consumed 26.47 times less energy as compared with the DTMS. For the same case at the responder end, the GTMS scheme consumed 5.11 times less energy as compared with the DTMS. This significant energy saving is only because the size of trust vector is depended on the size of the cluster. As we increase the number of clusters in the network, the average number of nodes in the cluster will decrease. If the numbers of nodes in the cluster become small then the size of trust vector will also reduce, which will take less transmission and reception power during transfer from a node to the cluster head.

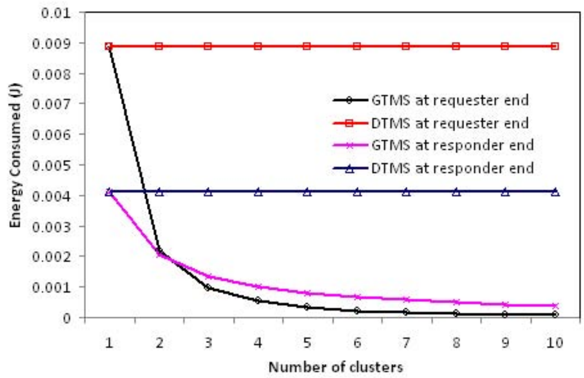


Figure 5. Energy Consumption: N=100, d=150

D. Scenario 4: Global trust value of each cluster

In order to calculate the global trust state (e.g. trusted, uncertain or un-trusted) of each member node, cluster head periodically broadcast a request message. In response all member nodes send back a trust state of other nodes to the cluster head. This approach, help cluster head to detect the presence of any malicious node in the group.

Whenever a base station needs a trust vector from the cluster heads it will send the request packet to all the cluster heads. In response all cluster heads will send the response packet to the base station. Since, the base station does not have any resource constraint problem, therefore, we have focused only on the energy consumption of the cluster heads. The total energy consumed at the responder (cluster head) end is:

$$E = E_{elec} \times 1 + [(8 + 24v) \times (E_{elec} + E_{amp} \times d^2)] \quad (19)$$

In the case of the GTMS $v \leq |G| - 1$, where $|G|$ is the number of groups in the network. In the case of the DTMS $v \leq N-1$, where N is the number of nodes in the network.

Comparison of both the schemes is shown in Figure 6. For the scenario of 100 nodes comprises of 10 equal size clusters, the GTMS consumed approximately 10.64 times less transmission and reception power as compared with the DTMS.

E. Summary

The GTMS scheme is invariant of any specific radio technology. The energy consumption analysis presented above, is just a single application of first order radio model proposed by H. O. Tan and I. Korpeoglu in [16].

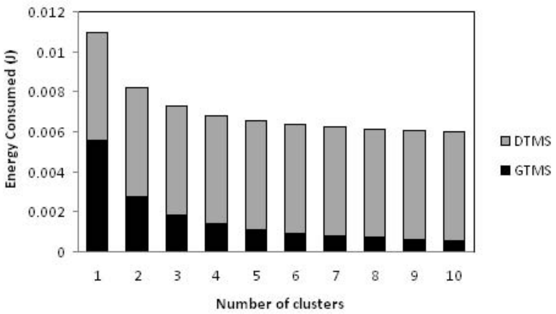


Figure 6. Energy Consumption: N=100, d=150

TABLE VI.
SUMMARY

Scenario	Node	Equation	Scaling factor
Scn-1	CH	$E_{T_x}(k,d) + r \times E_{R_x}(k')$	$r_{GTMS} \le r_{DTMS}$; $k'_{GTMS} \le k'_{DTMS}$
	SN	$E_{R_x}(k) + E_{T_x}(k',d)$	$k'_{GTMS} \le k'_{DTMS}$
Scn-2	SN	$j \times [E_{T_x}(k,d) + E_{R_x}(k')]$	$j_{GTMS} \le j_{DTMS}$
Scn-3	CH	$E_{T_x}(k,d) + E_{R_x}(k')$	-
Scn-4	CH	$E_{R_x}(k) + E_{T_x}(k',d)$	$k'_{GTMS} \le k'_{DTMS}$

The GTMS scheme never consume more energy than the DTMS scheme as shown in Table VI. In a worst case scenario, when the number of nodes in a cluster is equal to the number of nodes in the network, than the energy consumption of both schemes remain same. In other cases, the GTMS scheme always consume less energy than the DTMS scheme.

IV. Simulation-based Analysis and Evaluation

A. Simulation Environment

We have performed simulation using Sensor Network Simulator and Emulator (SENSE) [23]. For simulation purposes we have deployed a sensor network comprises of 225 sensor nodes that are spread in $800m \times 800m$ terrain. The network is divided into 16 equal size clusters. All sensor nodes are static and are organized in a grid fashion. Base station is located at the middle of the $800m \times 800m$ terrain. At the application layer, we have used our proposed TExP protocol [10] that is used to exchange the trust values between communicating nodes in an efficient manner. Format of TExP protocol is shown in Figure 7. Like [10], we used free space wireless channel, IEEE 802.11 MAC protocol, and a simplified version of DSR routing protocol (without route repairing). The rest of the specifications of a sensor node are defined in Table VII.

B. Comparison

For comparison purpose, we have implemented two protocols: GTMS and RFSN. We did not implement the PLUS scheme because it works on the top of its own defined routing protocol called PLUS_R. Whereas, GTMS and RFSN can works on the top of any routing protocol. For routing purposes, we used DSR routing protocol as mentioned earlier.

Source ID	Dest. ID	Protocol ID	Type	Payload	Send Time
2 bytes	2 bytes	1 byte	1 byte	variable	4 bytes

Figure 7. TExP packet format

TABLE VII.
Sensor Node's Specifications [10]

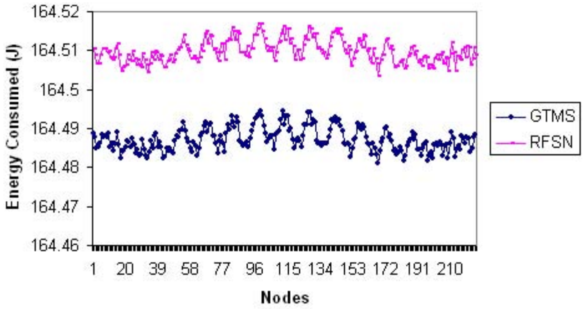
Initial battery of each sensor node	$1 \times 10^6 J$
Power consumption for transmission	1.6W
Power consumption for reception	1.2W
Power consumption in idle state	1.15W
Transmission power of the antenna	0.0280
Transmission and Reception gain	1.0
Carrier sense threshold	$3.652e^{-10}W$
Receive power threshold	$1.559e^{-11}W$

1) Scenario 1 [Peer recommendation of SNs]: During simulation, in each cluster, random number of source nodes are selected which perform peer recommendation. Also, each source node will get recommendations from random number of trusted nodes. Figure 8(a) shows that the GTMS consumed less energy then the RFSN scheme and the energy consumption difference approximately remains same (as shown in Figure 8(b)) for all 10 simulation runs. Therefore, we conclude that 10 simulation runs can give us reliable results.

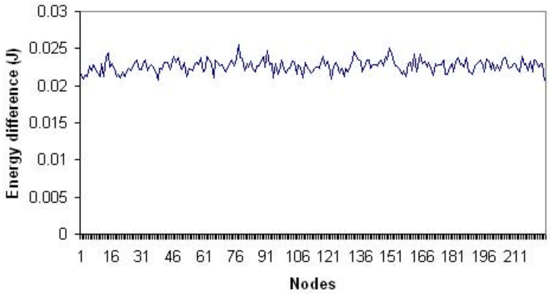
2) Scenario 2 [Peer recommendation of CHs]: During simulation, each cluster head performed peer recommendation with its neighboring clusters only. Here, also random number of peer recommendation will be perform by each cluster head and also random number of trusted neighboring cluster heads are selected for receiving recommendations. The average energy consumption for this scenario is shown in Figure 9(a), which shows that the GTMS scheme consumed much more less energy then the RFSN scheme. As Figure 9(b) shows that the energy difference between the GTMS and RFSN scheme is approximately 30.4J.

3) Complete Peer recommendation scenario: In practical, the frequency of peer recommendations within a cluster is much higher then the peer recommendation occurs between cluster heads. In order to get clear picture regarding the energy consumption, we have combined both scenarios. Where each sensor node performed peer recommendation with trusted member nodes and each cluster head performed peer recommendation with trusted neighboring cluster heads. Average energy consumed during complete peer recommendation scenario is shown in Figure 10. This figure shows that the GTMS scheme save significant amount of energy of approximately 1.58J as compared with the RFSN scheme.

Scenarios three and four presented in a previous section

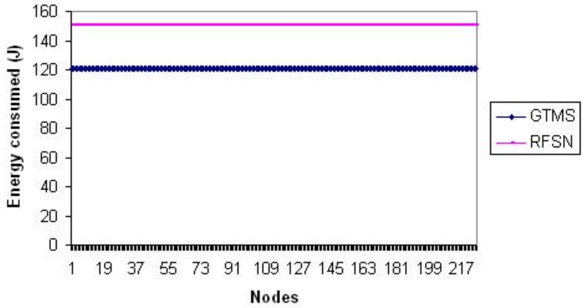


(a) Average energy consumption

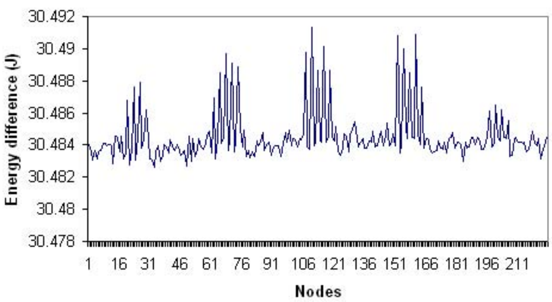


(b) Average energy consumption difference

Figure 8. Average energy consumption analysis for scenario 1 (10 simulation runs)



(a) Average energy consumption



(b) Average energy consumption difference

Figure 9. Average energy consumption analysis for scenario 2 (10 simulation runs)

are only applicable to the GTMS scheme. In both scenarios, the frequency of request and response packets is very low. Because packets are not forwarded very frequently

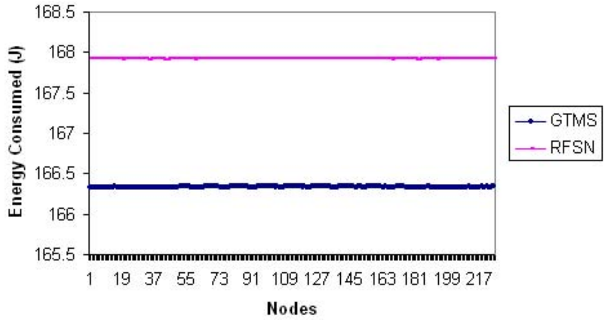


Figure 10. Average energy consumption analysis during complete peer recommendation (10 simulation runs)

rather packets are forwarded periodically. Therefore, even if we include both scenarios it will not effect much on net energy consumption of a whole network.

V. Conclusion

In this paper, we have presented the energy consumption analysis and evaluation of existing reputation-based trust management schemes of wireless sensor network. This sort of comparative study is currently not available in the literature. In this paper, we have evaluated theoretical energy consumption of three state-of-the-art reputation-based trust management schemes such as GTMS, RFSN and PLUS. Results show that, in a peer recommendation scenario, the GTMS consume less energy as compared with the PLUS and RFSN schemes. Additionally, we have also provided simulation-based analysis and evaluation which confirms our results obtain from theoretical analysis.

References

[1] T. Grandison and M. Sloman, “A survey of trust in internet applications,” *IEEE Comm. Surveys & Tutorials*, vol. 3, no. 4, 2000.
[2] S. Ganeriwal and M. B. Srivastava, “Reputation-based framework for high integrity sensor networks,” in *Proc. of ACM Security for Ad-hoc and Sensor Networks*, Oct. 2004.
[3] P. Resnick, R. Zeckhauser, E. Friedman, and K. Kuwabara, “Reputation systems: Facilitating trust in internet interactions,” *Comm. of the ACM*, vol. 43, no. 12, pp. 45–48, 2000.
[4] G. Theodorakopoulos and J. S. Baras, “On trust models and trust evaluation metrics for ad hoc networks,” *IEEE J. on Selected Areas in Comm.*, vol. 24, no. 2, pp. 318–328, Feb. 2006.
[5] Y. L. Sun, W. Yu, Z. Han, and K. J. R. Liu, “Information theoretic framework of trust modeling and evaluation for ad hoc networks,” *IEEE J. on Selected Areas in Comm.*, vol. 24, no. 2, pp. 305–317, Feb. 2006.
[6] S. Buchegger and J.-Y. L. Boudec, “A robust reputation system for peer-to-peer and mobile ad-hoc networks,” in *Proc. of P2PEcon*, Harvard University, Cambridge MA,USA, June 2004.
[7] M. Gupta, P. Judge, and M. Ammar, “A reputation system for peer-to-peer networks,” in *Proc. of the 13th Int. workshop on Network and operating systems support for digital audio and video*, Monterey, CA, USA, June 2003, pp. 144–152.

[8] D. Ingram, "An evidence based architecture for efficient, attack-resistant computational trust dissemination in peer-to-peer networks," in *Proc. of 3rd Int. Conf. on Trust Management*, ser. LNCS, vol. 3477. Paris: Springer-Verlag, May 2005, pp. 273–288.

[9] L. Xiong and L. Liu, "Peer trust: Supporting reputation-based trust for peer-to-peer electronic communities," *IEEE Trans. on Knowledge and Data Engineering*, vol. 16, no. 7, pp. 843–857, 2004.

[10] R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, S. Lee, and Y.-J. Song, "Group-based trust management scheme for clustered wireless sensor networks," *IEEE Transaction on Parallel and Distributed Systems (in press)*.

[11] S. Buchegger and J.-Y. L. Boudec, "Self-policing mobile ad hoc networks by reputation systems," *IEEE Comm. Magazine*, vol. 43, no. 7, pp. 101–107, July 2005.

[12] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Chapter 16: Wireless sensor network security: A survey," in *Security in Distributed, Grid, and Pervasive Computing*, Y. Xiao, Ed. CRC Press, 2006, pp. 367–410.

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

[14] Z. Yao, D. Kim, and Y. Doh, "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.

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

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

[17] H. sook Kim and K. jun Han, "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.

[18] A. Wesnarat and Y. Tipsuwan, "A power efficient algorithm for data gathering from wireless water meter networks," in *Proc. of the IEEE Int. Conference on Industrial Informatics*, Aug. 2006, pp. 1024–1029.

[19] S. Hussain and O. Islam, "An energy efficient spanning tree based multi-hop routing in wireless sensor networks," in *Proc. of the IEEE Wireless Communications and Networking Conference (WCNC 2007)*, March 2007, pp. 4383–4388.

[20] Y. Massad, M. Goyeneche, J. Astrain, and J. Villadangos, "Data aggregation in wireless sensor networks," in *Proc. of the 3rd Int. Confernence on Information and Communication Technologies: From Theory to Applications (ICTTA 2008)*, April 2008, pp. 1–6.

[21] L. Bai, L. Zhao, and Z. Liao, "Energy balance in co-operative wireless sensor network," in *Proc. of the 14th European Wireless Conference (EW 2008)*, June 2008, pp. 1–5.

[22] X. Lu, M. Spear, K. Levitt, and S. F. Wu, "Non-uniform entropy compression for uniform energy distribution in wireless sensor networks," in *Proc. of the 2008 2nd Int. Conference on Sensor Technologies and Applications (SENSORCOMM '08)*. Washington, DC, USA: IEEE Computer Society, 2008, pp. 723–731.

[23] (2008) B. K. Szymanski, SENSE: Sensor network simulator and emulator. [Online]. Available: http://www.ita.cs.rpi.edu/sense/index.html

Riaz Ahmed Shaikh received his B.S. degree in Computer Engineering from Sir Syed University of Engineering and Technology (SSUET), Karachi, Pakistan, in 2003, and his M.S. degree in Information Technology from National University of Sciences and Technology (NUST), Rawalpindi, Pakistan, in 2005. He received his Ph.D. degree from the Dept. of Comp. Eng., Kyung Hee University, Suwon, South Korea, in August 2009. His research interests include privacy, security and trust management. He is a professional member of the ACM. More information about him is available at http://member.acm.org/ riaz289.

Young-Koo Lee received his B.S., M.S. and PhD degrees in Computer Science from Korea Advanced Institute of Science and Technology(KAIST), Daejeon, Korea, in 1992, 1994 and 2002 respectively. From 2002 to 2004, he was a Post Doctoral Fellow at Advanced Information Technology Research Center (AITrc), KAIST, Korea, and a Postdoctoral Research Associate at Dept. of Computer Science, University of Illinois at Urbana-Champaign, USA. He has been a Assistant professor in the Dept. of Computer Engineering, Kyung Hee University, Korea since 2006. His current research focuses on Ubiquitous Data Management, Data Mining, Activity Recognition, Bioinformatics, On-line Analytical Processing (OLAP), Data Warehousing, Database Systems, Spatial Databases, Access Methods.

Sungyoung Lee received his B.S. from Korea University, Seoul, Korea. He got his M.S. and PhD degrees in Computer Science from Illinois Institute of Technology (IIT), Chicago, Illinois, USA in 1987 and 1991 respectively. He has been a professor in the Dept. of Computer Engineering, Kyung Hee University, Korea since 1993. He is a founding director of the Ubiquitous Computing Laboratory, and has been affiliated with a director of Neo Medical ubiquitous-Life Care Information Technology Research Center, Kyung Hee University since 2006. Before joining Kyung Hee University, he was an assistant professor in the Dept. of Comp. Sci., Governors State University, Illinois, USA from 1992 to 1993. His current research focuses on Ubiquitous Computing and applications, Context-aware Middleware, Sensor Operating Systems, Real-Time Systems and Embedded Systems. He is a member of the ACM and IEEE.