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

Riaz Ahmed Shaikh
Dept. of Comp. Eng.,
Kyung Hee University,
Global Campus, Korea
riaz@khu.ac.kr

Young-Koo Lee
Dept. of Comp. Eng.,
Kyung Hee University,
Global Campus, Korea
yklee@khu.ac.kr

Sungyoung Lee*
Dept. of Comp. Eng.,
Kyung Hee University,
Global Campus, Korea
sylee@oslab.khu.ac.kr

ABSTRACT

Energy consumption is one of the most important parameters for evaluation of a scheme proposed for 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 filled this gap by first proposing Generic Communication Protocol (GCP) that is used to exchange trust values. Based on this proposed GCP protocol, we have presented a theoretical energy consumption analysis and evaluation of three state-of-the-art reputation-based trust management schemes of WSNs.

Categories and Subject Descriptors

C.2 [**Computer Communication Networks**]: Network Protocols

General Terms

Measurement, Performance

Keywords

Reputation, Sensor networks, Trust management, Trust evaluation

*Corresponding Author.

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)Ť(IITA-2008-C1090-0801-0002) and by the MIC (Ministry of Information and Communication), Korea, Under the ITFSIP (IT Foreign Specialist Inviting Program) supervised by the IITA (Institute of Information Technology Advancement, C1012-0801-0003. Also, this work is financially supported by the Ministry of Education and Human Resources Development (MOE), the Ministry of Commerce, Industry and Energy (MOCIE) and the Ministry of Labor (MOLAB) through the fostering project of the Lab of Excellency.

ICUIMC-09, January 15-16, 2009, Suwon, S. Korea

1. 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" [3]. 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 [6], ad-hoc networks [9], and peer-to-peer networks [4]. In this paper, we will discuss them from the perspective of wireless sensor networks (WSNs).

Wireless sensor networks comprises of resource constraint devices having limited memory, energy and computation power. Many reputation-based trust management schemes [2, 1, 11, 7] 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 energy consumption analysis and evaluation of three state-of-the-art reputation-based trust management schemes. In order to perform this evaluation, we have propose a simple lightweight communication protocol for the exchange of trust values between communicating nodes in an efficient manner.

The rest of the paper is organized as follows: Section 2 contains description of proposed Generic Communication Protocol (GCP) and other existing trust management schemes. Section 3 presents energy consumption analysis and evaluation and section 4 concludes the paper.

2. DESCRIPTION OF PROTOCOLS

In order to calculate the energy consumption, firstly we must have the information about the number of bits transmitted and received during trust evaluation phase in different nodes. The number of bits are calculated by looking at specific communication protocols. For that purpose, we propose Generic Communication Protocol (GCP) that is used to transmit trust values between different nodes.

Basic packet format of the GCP is shown in Figure 1. In which ID_{src} represents identity of the source node, which consists of two bytes [5], [8]. ID_{dest} is the identity of the

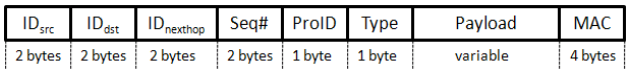


Figure 1: GCP packet format

Table 1: Packets of RFSN scheme

Type	Payload	Size
Req	ID of evaluating node (2 bytes)	16 bytes
Rep	ID of evaluating node(2 bytes), trust value(4 bytes)	20 bytes

destination node. $ID_{nexthop}$ is the identity of the next hop. Seq# represents the sequence number of the packet. ProtID represents the identity of the trust management protocol e.g. RFSN [2], PLUS [11] etc. Type field identify the type of the packet like request, response etc. Payload field is of variable size and contains the data specific to the type and protocol, such as trust value, identity of evaluating node (ID_{eval}) etc. MAC is the Message Authentication Code used to check the authenticity and integrity of the packet. The size of MAC field is 4 bytes.

2.1 RFSN Protocol

S. Ganeriwal and M. B. Srivastava [2] 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. 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 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 1.

2.2 PLUS Protocol

Z. Yao et al. [11] 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. 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 2.

2.3 GTMS Protocol

Table 2: Packets of PLUS scheme

Type	Payload	Size
EReq	ID of evaluating node (2 bytes)	16 bytes
ERep	ID of evaluating node(2 bytes), trust value(4 bytes)	20 bytes
EInf	ID of evaluating node(2 bytes), Error code(2 bytes)	18 bytes
EAck	ID of evaluating node (2 bytes)	16 bytes
EArg	ID of evaluating node (2 bytes), trust value(4 bytes)	20 bytes

Shaikh R.A. et. al. [7] have proposed lightweight Group-based Trust Management Scheme (GTMS) for WSNs. It uses hybrid trust management approach which reduces the cost of trust evaluation. The GTMS scheme is comprises of four pairs of request and response packets as shown in Table 3.

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 16 bytes to node y. In response, node y send a response packet (iTRep) of size 17 bytes to node x. iTRep contains the trust value of z.

Pair 2: used for the transfer of trust vector from node to CH. After a periodic interval, the CH j broadcast a request (iVReq) packet of size 14 bytes inside the group. In response all nodes that belongs the cluster j send back a response packet (iVRep) of size $15 + 2.25v$ bytes, where $v \leq n - 1$ represents the length of the trust vector.

Pair 3: used for getting recommendation from BS by CH. Whenever a CH j need a recommendation from the BS about another cluster k, it send a request packet (oTReq) of size 16 bytes to the BS. In response, BS send a response packet (oTRep) to the CH j that contain the trust value of CH k. Size of the response packet is 17 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 of size 16 bytes. In response, all CHs send back a response packet (oVRep) of size $15 + 3v$ bytes, where $v \leq |G|$ represents the length of the trust vector.

3. ANALYSIS AND EVALUATION

For the energy consumption analysis, we assume first order radio model, 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 [10] is:

$$\begin{aligned} E_{Tx}(k,d) &= kE_{elec} + kd^2E_{amp} \\ E_{Rx}(k) &= kE_{elec} \end{aligned} \quad (1)$$

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 $100pJ/bit/m^2$.

By using GCP communication protocol, we have performed the analysis of energy consumption of various trust management schemes in different scenarios.

Table 3: Packets of GTMS scheme

		Type	Payload	Size (bytes)
packets move inside cluster	Pair 1: for peer recommendation	iTReq (SN-SN)	ID of evaluating node (2 bytes)	16
		iTRep (SN-SN)	ID of evaluating node (2 bytes), trust value (1 byte)	17
	Pair 2: for transfer of trust vector	iVReq (CH-SN)	Nil	14
		iVRep (SN-CH)	Vector length v(1 byte), ID (2 bytes) and trust state (1 bit) of v member nodes	15+2.25v
packets move outside cluster	Pair 3: for peer recommendation	oTReq (CH-BS)	ID of evaluating node (2 bytes)	16
		oTRep (BS-CH)	ID of evaluating node (2 bytes), trust value (1 byte)	17
	Pair 4: for transfer of trust vector	oVReq (BS-CH)	Nil	14
		oVRep (CH-BS)	Vector length v(1 byte), ID (2 bytes) and trust value (1 byte) of other clusters	15+3v

3.1 Scenario 1

When a SN needs a recommendation about other nodes, it will send a request packet to its peers. In the case of GTMS, 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, $0 < j \leq n-2$, and n is the number of nodes in the group. For peer recommendation, the size of a request packet is 16 bytes, thus $k = 128$ bits. The size of a response packet is 17 bytes, thus $k' = 136$. So the total energy consumed at the requester end is:

$$\begin{aligned} E &= j\left[E_{Tx}(128,d) + E_{Rx}(136)\right] \\ E &= j\left[128(E_{elec} + d^2E_{amp}) + (136E_{elec})\right] \end{aligned} \tag{3}$$

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

$$\begin{aligned} E &= E_{Rx}(128) + E_{Tx}(136,d) \\ E &= 128E_{elec} + 136(E_{elec} + d^2E_{amp}) \end{aligned} \tag{4}$$

Energy consumption during peer recommendation of other schemes is shown in Table 4. In the case of RFSN, the energy consumption at the requester end is:

$$E = t \times \left[E_{Tx}(128,d) + E_{Rx}(160)\right] \tag{5}$$

where t represents the number of trusted node in the cluster ($0 < t \leq n-2$), 128 and 160 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:

$$\begin{aligned} E &= E_{Rx}(128) + E_{Tx}(160,d) \\ E &= 128E_{elec} + 160(E_{elec} + d^2E_{amp}) \end{aligned} \tag{6}$$

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

$$\begin{aligned} E &= E_{Tx}(128,d) + (n-2)E_{Rx}(160) \\ E &= 128(E_{elec} + d^2E_{amp}) + (n-2)(160E_{elec}) \end{aligned} \tag{7}$$

Here 128 and 160 represents the size of the request and response packets of PLUS scheme respectively. Also for the PLUS, the energy consumed at the responder end is:

$$\begin{aligned} E &= E_{Rx}(128) + E_{Tx}(160,d) \\ E &= 128E_{elec} + 160(E_{elec} + d^2E_{amp}) \end{aligned} \tag{8}$$

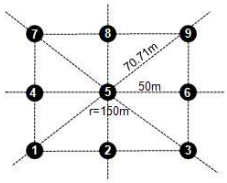


Figure 2: Sample Group Scenario

In order to compare the energy consumption during peer recommendation scenario, we have assumed that a single group consists of nine nodes arranged in a grid fashion as shown in Figure 2. 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 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 3(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 3(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.

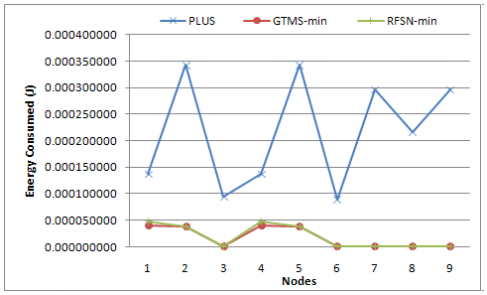
Scenario 2, 3 and 4 are only applicable to the GTMS scheme. Therefore, we have compared the GTMS scheme with the generic Distributed Trust Management Scheme (DTMS) in which each node maintains a one-to-one trust relationship with each other.

3.2 Scenario 2

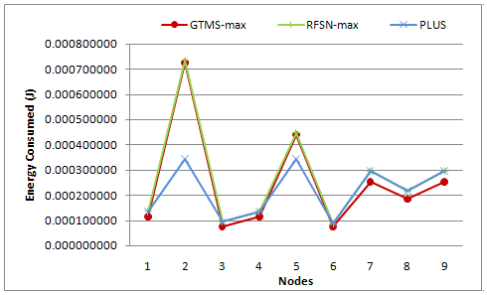
Whenever a sensor node gets request to send trust vector from the cluster head, it will send $n-1$ bytes of trust vector data to the cluster head. Here n is the number of nodes

Table 4: Parameters for one peer recommendation request in 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	128 bits	128 bits	128 bits
Size of response packet	136 bits	160 bits	160 bits
Energy consumption at requester	$j[E_{T_x}(128,d)+E_{R_x}(136)]$	$t[E_{T_x}(128,d)+E_{R_x}(160)]$	$E_{T_x}(128,d)+(n-2)\times E_{R_x}(160)$
Energy consumption at responder	$E_{T_x}(136,d)+E_{R_x}(128)$	$E_{T_x}(160,d)+E_{R_x}(128)$	$E_{T_x}(160,d)+E_{R_x}(128)$



(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 3: Energy consumption during peer recommendation scenario

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:

$$E = E_{T_k}(k,d) + \sum_{j=0}^{r} E_{R_x}(k') \tag{9}$$

$$E = k \times (E_{elec} + E_{amp} \times d^2) + \sum_{j=0}^{r} E_{elec} \times k' \tag{10}$$

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. The size of the request packet is 112 bits and size of the response packet is $120+18v$.

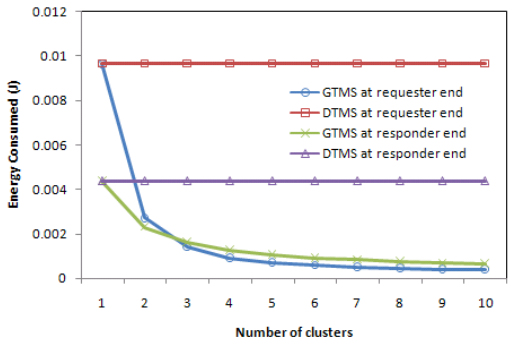


Figure 4: Energy Consumption: N=100, d=150

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

$$E = 112 \times (E_{elec} + E_{amp} \times d^2) \ + \sum_{j=0}^{r} E_{elec} \times (120 + 18v) \tag{11}$$

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:

$$E = E_{elec} \times k + k' \times (E_{elec} + E_{amp} \times d^2) \tag{12}$$

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

$$E = E_{elec} \times 112 + (120 + 18v) \times (E_{elec} + E_{amp} \times d^2) \tag{13}$$

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 4. 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 that case energy consumption at the requester and responder ends are same. But as we increase the number of clusters in the net-

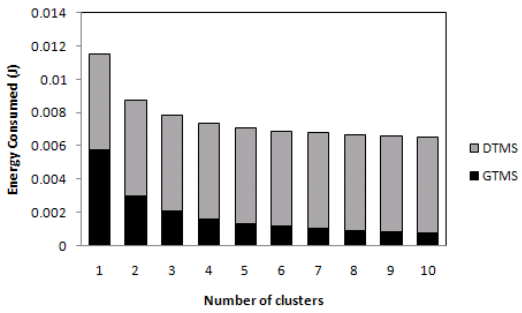


Figure 5: Energy Consumption: N=100, d=150

work, GTMS shows lower energy consumption as compared to the DTMS. For example, for the case of ten clusters in the network comprises of 100 nodes, at the requester end, the GTMS scheme consumed 25.15 times less energy as compared to the DTMS. For the same case at the responder end, the GTMS scheme consumed 6.69 times less energy as compared to 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.

3.3 Scenario 3

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. The total energy consumed at the cluster head will be;

$$E = 128 \times (E_{elec} + E_{amp} \times d^2) + E_{elec} \times 136 \qquad (14)$$

where 128 bits represents the size of the request packet and 136 is the size of the response packet. This equation will remain same for the DTMS and GTMS both.

3.4 Scenario 4

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:

$$E = E_{elec} \times 112 + [(120 + 24 \times v) \times (E_{elec} + E_{amp} \times d^2)] \quad (15)$$

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 5. For the scenario of 100 nodes comprises of 10 equal size clusters, GTMS consumed approximately 7.38 times less transmission and reception power as compared to the DTMS.

4. 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 proposed generic communication protocol that is used to exchange trust values. Based on this GCP protocol, 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 to the PLUS and RFSN schemes.

5. REFERENCES

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

[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*, pages 66–67, Oct. 2004.

[3] T. Grandison and M. Sloman. A survey of trust in internet applications. *IEEE Comm. Surveys & Tutorials*, 3(4), 2000.

[4] 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*, pages 144–152, Monterey, CA, USA, June 2003.

[5] C. Karlof, N. Sastry, and D. Wagner. TinySec: a link layer security architecture for wireless sensor networks. In *Proc. of the 2nd Int. Conf. on Embedded networked sensor systems*, pages 162–175, Baltimore, MD, USA, Nov. 2004.

[6] P. Resnick, R. Zeckhauser, E. Friedman, and K. Kuwabara. Reputation systems: Facilitating trust in internet interactions. *Comm. of the ACM*, 43(12):45–48, 2000.

[7] 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. *will be published in IEEE Transaction on Parallel and Distributed Systems.*

[8] R. A. Shaikh, S. Lee, M. A. U. Khan, and Y. J. Song. LSec: Lightweight security protocol for distributed wireless sensor network. In *11th IFIP Int. Conf. on Personal Wireless Comm., LNCS 4217*, pages 367–377, Albacete, Spain, Sept. 2006.

[9] 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.*, 24(2):305–317, Feb. 2006.

[10] H. O. Tan and I. Korpeoglu. Power efficient data gathering and aggregation in wireless sensor networks. *ACM SIGMOD Record*, 32(4):66–71, Dec. 2003.

[11] 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 Ad-hoc and Sensor Systems*, pages 437–446, Vancouver, Canada, Oct. 2006.