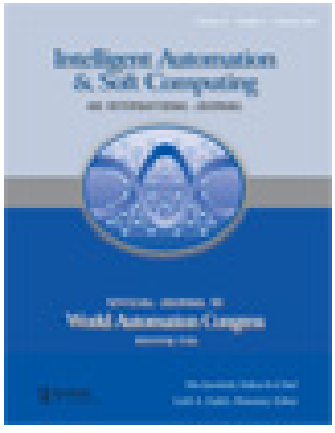


Intelligent Automation & Soft Computing
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/tasj20

Security Completeness Problem in Wireless Sensor Networks

Riaz Ahmed Shaikh[a], Sungyoung Lee[b] & Aiiad Albeshri[a]
[a] Department of Computer Science, King Abdulaziz University, Jeddah, Saudi Arabia
[b] Department of Computer Engineering, Kyung Hee University, Yongin-Si, Korea
Published online: 25 Nov 2014.

Intelligent Automation and Soft Computing, 2014
http://dx.doi.org/10.1080/10798587.2014.970345

SECURITY COMPLETENESS PROBLEM IN WIRELESS SENSOR NETWORKS

Riaz Ahmed Shaikh[1], Sungyoung Lee*[2], Aiiad Albeshri[1]
[1]*Department of Computer Science, King Abdulaziz University, Jeddah, Saudi Arabia*
[2]*Department of Computer Engineering, Kyung Hee University, Yongin-Si, Korea*

ABSTRACT—With the emergence of wireless sensor networks and its usage in sensitive monitoring and tracking applications, the need of ensuring complete security is gaining more importance than ever before. Complete security can only be ensured by adding privacy, cryptographic-based security and trust management aspects in a security solution. However, integration of all these three aspects in a single solution for resource constraints wireless sensor networks is not trivial. Current research intensively focuses on all these three aspects in an isolated manner. To the best of our knowledge, we have not found any work in the literature that comprehensively discusses: how these various privacy, security and trust solutions work together? In this work, we have made the first step towards this direction and to show how integration of various privacy, security and trust solutions can be performed in a single solution in step-by-step manner.

Key Words: Privacy; Security; Trust; Wireless sensor networks

1. INTRODUCTION

In this work, we have made the first step towards this direction and to show how integration of various privacy, security and trust solutions can be performed in a single solution in step-by-step manner. Many researchers from academia and industry are actively doing research in the domain of privacy (Chai, Xu, Xu, & Lin, 2012; Haowen Chan & Perrig, 2003; Jian, Chen, Zhang, & Zhang, 2007; Li, Li, Ren, & Wu, 2012; Shaikh et al., 2010), security (Ahmed, Huang, & Sharma, 2012; Oliveira et al., 2011; Perrig, Stankovic, & Wagner, 2004; Shaikh, Lee, Khan, & Song, 2006), and trust (Feng, Che, Wang, & Yu, 2013; Ganeriwal, Balzano, & Srivastava, 2008; Gómez Mármol & Martínez Pérez, 2011; Shaikh et al., 2009; Yu, Li, Zhou, & Li, 2012) in wireless sensor networks (WSNs). Integration of privacy, security and trust solutions are utmost necessary in achieving completeness in the security solution. Let us take an example of the battlefield application as shown in the Figure 1. In this figure, typical sensor nodes are deployed to monitor the movement of the tanks and soldiers in the battlefield. In this example, there is one sink node which collects all the information forwarded by the sensor nodes. The sensor nodes, which detect the appearance of the tanks and / or soldiers will act as source nodes. They will forward this information to the sink node in multi-hop wireless communication fashion. This scenario is obviously unsafe, because an adversary can perform multiple malicious activities. For example,

- Can capture the packet and get access to sensitive information. In order to avoid this threat and to ensure data secrecy, the contents of the packets must be encrypted.

*Corresponding author. Email: sylee@oslab.khu.ac.kr

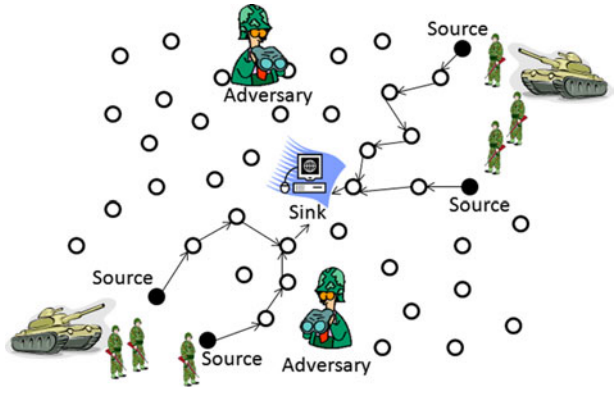


Figure 1. Sample Battlefield Application Scenario.

- Can easily locate the source by back tracing the packet transmissions hop-by-hop and to capture the soldiers. In order to avoid this threat, source location and route privacy must be ensured.
- He can take over the control of some sensor nodes in the field. With the help of malicious nodes, he can change or delete any critical information present in the packet. In order to avoid this threat, a trust management scheme should be deployed. It will ensure that the packets should reach to the destination by passing through trustworthy intermediate nodes.

Now let us take the example of habitat monitoring application scenario, such as, Great Duck Island (Mainwaring, Culler, Polastre, Szewczyk, & Anderson, 2002) or Save-the-panda application (Kamat, Zhang, Trappe, & Ozturk, 2005). In these applications, large numbers of sensor nodes are deployed to observe the vast habitat for ducks and pandas. From these examples one can see the need of all privacy, security and trust features in a single solution.

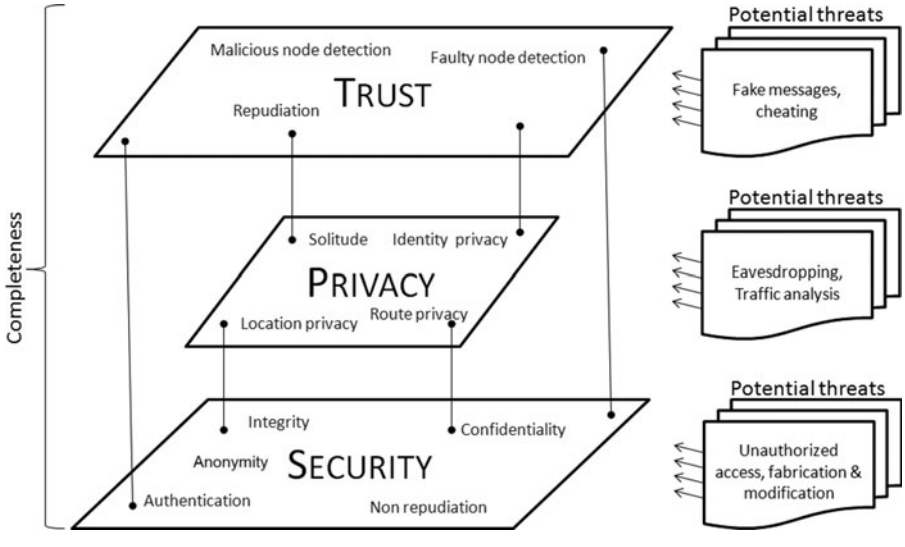


Figure 2. Complete Security Solution Perspective.

In the literature, various privacy, security and trust solutions exists that are used to provide protection against various types of attacks as shown in Figure 2. We have not found any solution or framework in the literature that comprehensively discusses how these various privacy, security and trust solutions work together. Also, we need to know whether the integrated solution meets the resource constraint requirements of the sensor networks or not.

In this work, a new integrated security framework for WSNs is presented as shown in Figure 3. This framework is built on top of individually proposed, mutually complementary trust (Shaikh et al., 2009), privacy (Shaikh et al., 2010), and security (Shaikh et al., 2006) solutions that closely interact with one another. In the trust component, the group-based trust management scheme (GTMS) (Shaikh et al., 2009) is responsible for calculating the trust values of sensor nodes. With the help of generic trust exchange communication protocol (TExP) (Shaikh et al., 2009), the GTMS module will exchange trust values with other nodes. These trust values are further used by the proposed routing schemes, such as, IRL (Shaikh et al., 2010) and r-IRL (Shaikh et al., 2010) that ensures identity, route and location privacy of the node. Trust values in these routing algorithms are used for the selection of reliable and secure communication path. If the malicious node is detected then the GTMS will send alert message to the lightweight security (LSec) protocol (Shaikh et al., 2006) that will take further protective steps, such as, deletion of a shared secret key, termination of any ongoing session with the malicious node, and send alert messages to other member nodes. The LSec protocol is used to generate shared secret keys. The secret keys are used by the different modules of the integrated solution to exchange information in an encrypted manner.

In this paper, theoretical analysis and evaluation of the complete integrated solution is presented. From communication overhead and memory consumption analysis perspective, we found that the proposed solution is lightweight. Therefore, it is practically feasible to use this solution in WSNs.

The rest of the paper is organized as follows: Section 2 presents an overview of the proposed privacy, security and trust components. Section 3 depicts the semantic layout of the proposed integrated solution. Section 4 provides theoretical analysis and evaluation of the proposed solution. Finally, Section 5 concludes the paper.

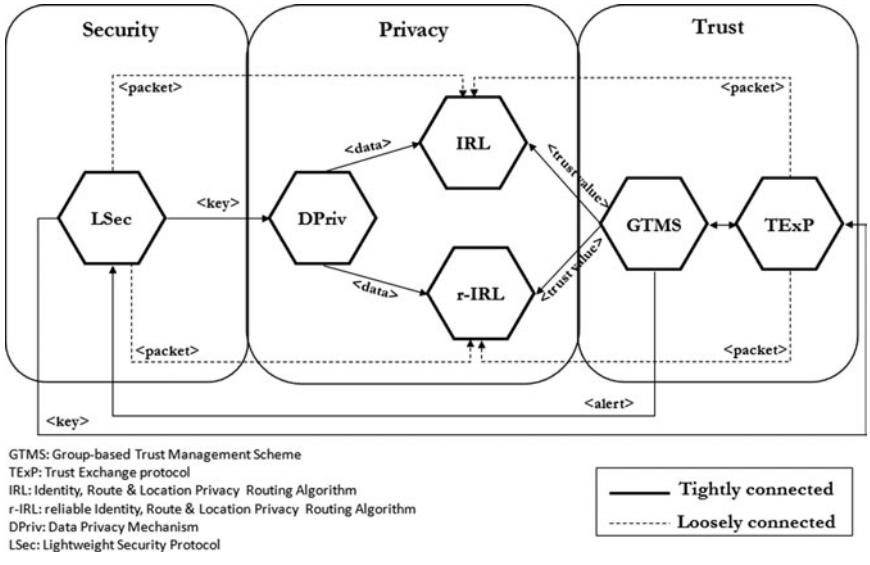


Figure 3. Integrated Privacy, Security and Trust Framework.

2. OVERVIEW OF PRIVACY, SECURITY AND TRUST SOLUTIONS

2.1 Trust Management

Various trust management schemes (Aivaloglou, Gritzalis, & Skianis, 2007; Boukerche, Xu, & El-Khatib, 2007; Duan, Yang, Zhu, Zhang, & Zhao, 2014; Feng et al., 2013; Ganeriwal et al., 2008; Ishmanov, Kim, & Nam, 2014; Li, Zhou, & Du, 2013; Liu, Abu-Ghazaleh, & Kang, 2007; Shaikh et al., 2009; Yao, Kim, & Doh, 2006; Yu et al., 2012) have been proposed for wireless sensor networks. Due to page limit restrictions, a brief overview and comparison of the existing trust management schemes is presented in Table I.

For demonstrating the complete integrated solution, the Group-based trust management scheme (GTMS) (Shaikh et al., 2009) is selected. It works in three phases.

First, each sensor in a group or cluster calculates individual trust values for all other nodes in the group. Trust is calculated by using either history of successful and unsuccessful interactions or by peer recommendations. Based on the trust values, each node will assign one of the three possible trust states (trusted, un-trusted, and uncertain) to the other nodes.

Second, each node forwards the trust state of all the group member nodes to the cluster head. Based on the received information, a cluster head detects the malicious nodes and send information to the base station. Also, cluster head keeps the record of interactions with other cluster heads. Based on that, trust value of other cluster heads is calculated. This information is forwarded to the base station on request.

Third, whenever the base station receives information from the cluster head about the member nodes, then it assigns one of the three possible states (trusted, un-trusted, and uncertain) to the whole group. This trust value can be used during communication between cluster heads.

2.2 Privacy

Relevant to proposed work, the privacy is categorized as: 1) Identity privacy, 2) route privacy, 3) location privacy, and 4) data privacy. A brief overview of existing privacy schemes (Chen & Lou, 2014; Jose & Princy, 2013; Kamat et al., 2005; Li & Ren, 2010; Misra & Xue, 2006; Ozturk, Zhang, & Trappe, 2004; Shaikh et al., 2010; Tan, Li, & Song, 2014; Wood, Fang, Stankovic, & He, 2006) with respect to the four privacy features is shown in Table II. This table shows that only IRL & r-IRL (Shaikh et al., 2010) schemes cover all four aspects.

For the purpose of a demonstration of complete integrated solution, Identity, Route, and Location (IRL) privacy algorithm (Shaikh et al., 2010) is selected. At the network layer, IRL algorithm ensures the anonymity of source nodes identity and location from the adversary. It also gives assurance that the packet will reach to its destination by passing through only trusted intermediate nodes. The brief description of the IRL algorithm is given below.

Based on the geographic location of the destination, a source node classifies its neighboring nodes into four categories that are forward, right backward, left backward, and middle backward directions, as shown in the Figure 4. Whenever a source node wants to forward the packet, it will first check the availability of the trusted nodes in its forward direction set. In the presence of the trusted nodes, it will randomly select one trusted node as a next hop from that set, and forward packet to it. If the trusted nodes are available, source node will randomly select one node as a next hop from these sets and forward packet to it. If the trusted node does not exist in these sets, then the source node will randomly select one trusted node from the backward middle set and forward the packet towards it. In case of packet drop, this information will be kept or sent to base station or not? That no trusted nodes are available?

An extension of the IRL algorithm entitled reliable IRL (r-IRL) could also be used at the network layer.

Table I. Comparison of Trust Management Solutions.

Scheme	Model	Approach	Trust-based on direct observations	Trust-based on indirect observations	Trust levels	Dependency on routing Scheme (RS)
TMS (Feng et al., 2013)	Fully Distributed	Behavior-based (BB)	Yes	Yes	3	Any
RFSN (Ganeriwal et al., 2008)	Fully Distributed	Behavior-based	Yes	Yes	2	Any
ATRM (Boukerche et al., 2007)	Localized Distributed	Certificate-based (CB)	Yes	No	–	Any clustered based RS
FTSN (Aivaloglou et al., 2007)	Hybrid	Combined BB & CB	Yes	Yes	2	Any
TSRF (Duan et al., 2014)	Fully Distributed	Behavior-based	Yes	Yes	3	TSRF Routing
Ishmanov et al. (Ishmanov et al., 2014)	Localized Distributed	Behavior-based	Yes	Yes	4	Any
LDTS (Li et al., 2013)	Hybrid	Behavior-based	Yes	Yes	–	Any clustered based RS
T-RGR (Liu et al., 2007)	Fully Distributed	Behavior-based	Yes	No	2	Any geographic Based RS
GTMS (Shaikh et al., 2009)	Hybrid	Behavior-based	Yes	Yes	3	Any clustered based RS
PLUS (Yao et al., 2006)	Fully Distributed	Behavior-based	Yes	Yes	4	PLUS_R
TMA (Zhang, Shankaran, Orgun, Varadharajan, & Sattar, 2010)	Hybrid	Combined BB & CB	Yes	Yes	–	Any clustered based RS

Table II. Comparison of Privacy Solutions.

	Identity privacy	Route privacy	Location privacy	Data privacy
Chen et al. (Chen & Lou, 2014)	No	Yes	Yes	NA
PEPPDA (Jose & Princy, 2013)	No	No	No	Yes
PSR (Kamat et al., 2005)	No	Yes	Yes	NA
RRIN (Li & Ren, 2010)	No	Yes	Yes	NA
SAS & CAS (Misra & Xue, 2006)	Yes	Depending on a routing scheme	Depending on a routing scheme	Yes
PFR (Ozturk et al., 2004)	No	Yes	Yes	NA
IRL & r-IRL (Shaikh et al., 2010)	Yes	Yes	Yes	Yes
EDROW (Tan et al., 2014)	No	Yes	Yes	NA
SIGF (Wood et al., 2006)	No	Yes	Yes	Yes

Data privacy is achieved in the following manner. The payload contains the identity of the source node and the actual data. Identity is encrypted with the public key of the base station and data is encrypted with the secret key shared between the sender node and the base station.

2.3 Security

In general, security can be discussed from five aspects: 1) Authentication, 2) Access Control, 3) Confidentiality, 4) Integrity, and 5) Availability. Qualitative comparison of existing security schemes from these aspects is given in Table III.

For the purpose of a demonstration, lightweight security protocol (LSec) (Shaikh et al., 2006) is used in the complete integrated solution. It provides support for both static and mobile environments, which may contain single and multiple base stations. It uses both symmetric and public key cryptography schemes for providing secure communication in sensor networks. It operates in the following three phases.

1. Authentication and authorization: It is performed during the exchange of *Request* and *Response* packets by using symmetric scheme.
2. Key distribution phase: It involves the sharing of random secret key in a secure manner by using

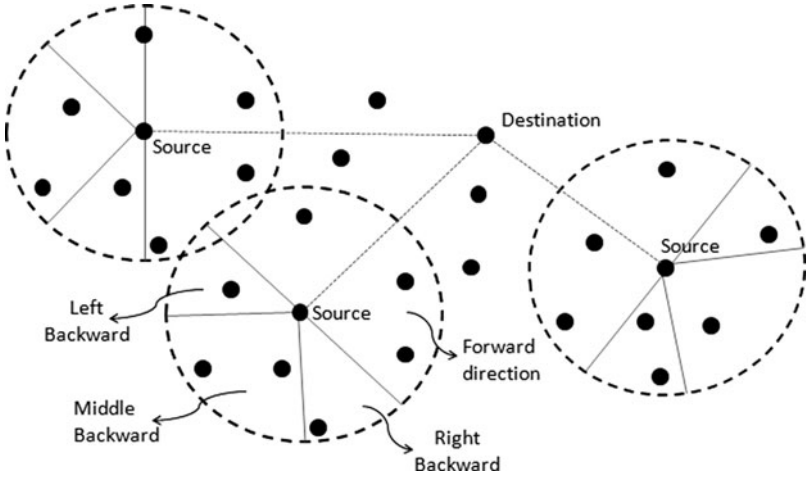


Figure 4. Sample IRL Node Classification.

Table III. Comparison of Security Solutions.

	Authentication	Access Control	Confidentiality	Integrity	Availability
LSec (Shaikh et al., 2006)	Yes	Yes	Yes	No	No
TuLP (Gong et al., 2014)	Yes	NA	NA	Yes	NA
Huang et al. (Huang et al., 2010)	Yes	No	Yes	Yes	No
TinySec (Karlof et al., 2004)	Yes	No	Yes	Yes	No
SMMR (Nguyen et al., 2014)	Yes	No	Yes	No	No
LiSP (Park & Shin, 2004)	Yes	Yes	Yes	Yes	Yes
SPINS (Perrig et al., 2002)	Yes	No	Yes	Yes	No
MUQAMI + (Syed et al., 2010)	Yes	No	Yes	Yes	No
LEAP + (Zhu et al., 2006)	Yes	No	Yes	Yes	No

public key cryptography scheme. In this phase *INIT* and *ACK* packets will be exchanged.

3. Data transmission phase: It involves the transmission of data packets in an encrypted manner by using symmetric cryptography scheme.

3. INTEGRATED SOLUTION

Developing an integrated security solution for wireless sensor network is not a trivial task (Boyle & Newe, 2008; Cionca, Newe, & Dădârlat, 2012). Some researchers (Cionca et al., 2012) have made a nice effort by developing a configuration tool that helps users to integrate various key management and encryption protocols in WSN applications. However, privacy and trust management features are not covered in their solution. In general, integrated security solutions are very beneficial to use in many real world applications, such as, the Kindergarten Safety System (Yang & Jung, 2010), and various Telemedicine aided by WSNs (Hsu et al., 2010).

In this section, we are presenting a schematic layout of the complete system based on the SENSE (Chen, Branch, Pflug, Zhu, & Szymanski, 2005) node architecture as shown in Figure 5. It shows the integration of all the components on a single sensor node. Figure 5(a) represents the schematic layout of proposed solution for the sensor nodes where the encryption facility is available as software. However, in order to strengthen the security, many vendors provide the support of hardware level encryption. For example, AES encryption module is available on the Chipcon CC2420 transceiver chip that is used in Crossbow MICAz and MoteIV's TmoteSKY (Healy, Newe, & Lewis, 2008). In order to ensure security and integrity of hardware, manufacture can utilize trusted computing platform (Kambourakis, Gritzalis, & Park, 2010). The proposed solution could also be used in such sensor nodes as shown in the Figure 5(b).

3.1 Interfaces of Trust Component

The proposed GTMS module has four external interfaces as shown in Figure 6.

1. *MAC interface:* From the MAC layer, the GTMS component receives link layer acknowledgment (ACK) and enhanced passive acknowledgment (P-ACK) for each transmitted packet. Based on this information, the GTMS module considers an interaction as a successful or an unsuccessful one. This information will be further recorded in the sliding time window. With this time window information, the time-based past interaction trust value of the other node is calculated.
2. *Network interface:* Whenever a routing protocol (e.g. IRL (Shaikh et al., 2010) or r-IRL (Shaikh et al., 2010)) needs to select trusted next hop node for the purpose of forwarding packets, it first interacts with the GTMS module. During the initialization phase, the IRL and r-IRL protocols

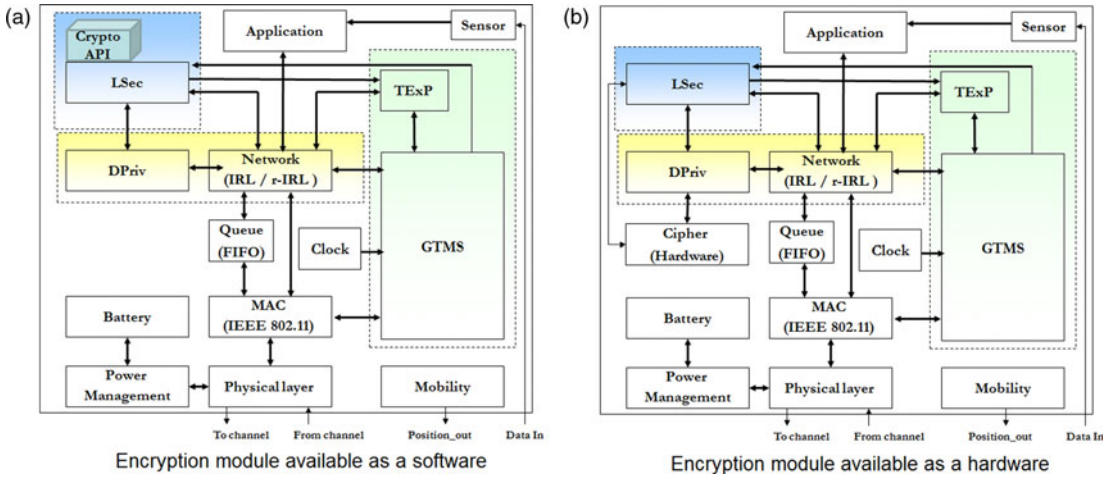


Figure 5. Schematic Layout of the System.

provide node identities to the GTMS module. The GTMS module informs the IRL and r-IRL protocols about the trusted neighbor nodes. Based on this information, the routing protocol makes reliable routing decisions.

3. *Exchange interface:* Whenever the GTMS module needs recommendations from other nodes, it sends request packets via generic Trust Exchange Protocol (TExP) (Shaikh et al., 2009). Based on the recommendation received via the TExP protocol, it computes the trust value.
4. *Alert interface:* Whenever the GTMS module detects any malicious node (Shaikh et al., 2009), it will send alert message to the security component.

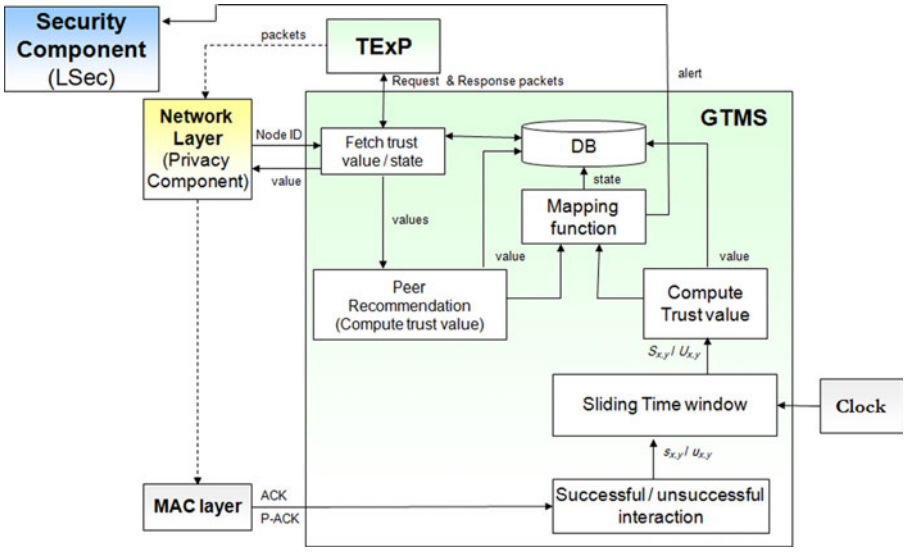


Figure 6. Interfaces of Trust Component.

3.2 Interfaces of Privacy Component

The privacy component is mainly used for routing. This component ensures the anonymity of a source node's identity and location from an adversary. It also takes care of route anonymity of data packets and data privacy. This privacy component has four external interfaces as shown in the Figure 7.

1. *Application interface:* First, it is connected to the application layer, from where it receives data packets for forwarding.
2. *Trust interface:* Second, it is connected with the trust component (Shaikh et al., 2009), which provides trust values of the neighboring nodes. These trust values are further used to make reliable routing decisions.
3. *Security interface:* Third, it is connected to the security component (Shaikh et al., 2006), which provides secret key that is used to perform encryption of the data packets.
4. *MAC interface:* Last, it is connected to the MAC layer, through which it sends and receives packets.

3.3 Interfaces of Security Component

The security component is mainly used to generate secret temporal session keys. It has four external interfaces as shown in the Figure 8.

1. *Key generation interface:* It is mainly used for the authorization and generation of secret session keys. Through this interface, security component send and receive *INIT*, *ACK*, *Request* and *Response* packets via network layer. In the proposed solution, it sends these packets via IRL (Shaikh et al., 2010) or r-IRL (Shaikh et al., 2010) privacy component.
2. *Cipher interface:* It is used to perform encryption and decryption of the data packets. In the proposed solution, it is connected with the data privacy (DPriv) module of the privacy component.
3. *Alert handler interface:* It is mainly used to receive alert messages. On the reception of an alert message, the security component will terminate earlier key and generate new ones if required. In the proposed solution, it receives alert messages from the trust component.

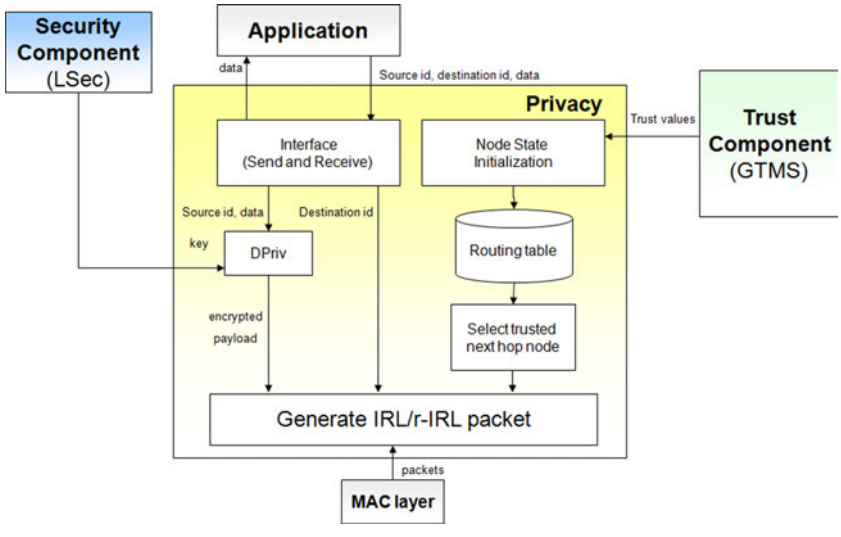


Figure 7. Interfaces of Privacy Component.

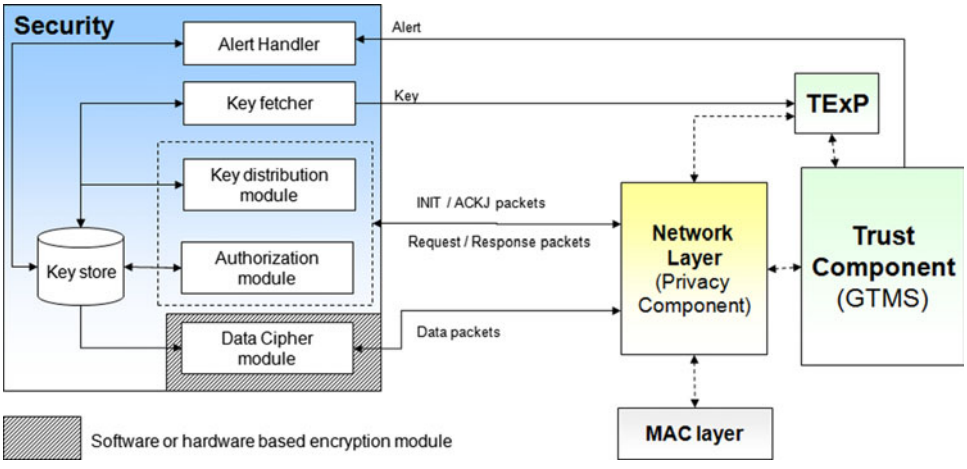


Figure 8. Interfaces of Security Component.

4. *Key provider interface:* It is used to provide secret keys (Shaikh et al., 2006) to other components. For example, it provides the secret key to the TExP module (Shaikh et al., 2009) of trust component.

4. THEORETICAL ANALYSIS AND EVALUATION

4.1 Memory Consumption Analysis

At each sensor node, the trust component needs $(n-1)(4+4\Delta t)$ memory space to store trust records. Here n represents the total number of nodes in the group and Δt represents the size of time window. For the privacy component, each sensor node needs $6.375n$ memory space and the security component requires 72 bytes of memory to store keys. Therefore, memory requirement of complete solution at each sensor node is:

$$M_{\mathrm{SN}} = (n-1)(4+4\Delta t) + 6.375n + 72 \tag{1}$$

This equation shows that the memory space at each sensor node mainly depended on the size of the cluster and the length of time window. However, the window length could be made shorter or longer based on the network analysis scenarios. Let us assume that the value of Δt is dependent on the size of the cluster. In this case, adaptive Δt could be calculated as the following.

$$\Delta t = \left\lceil \left| \frac{-6.375n - 72}{4(n-1)} - 1 \right| \right\rceil \tag{2}$$

At each cluster head, the trust component needs $(|G| + \sigma - 2)(4+4\Delta t)$ memory space to store trust records. Here |G| represent the total number of groups/clusters in the networks, and σ represents the average size of the cluster. Also, at each sensor node, privacy and security components requires $6.375n$ and 72 bytes of memory respectively. Therefore, memory requirement of the complete solution at each cluster head is:

$$M_{\mathrm{CH}} = (|G| + \sigma - 2)(4+4\Delta t) + 6.375n + 72 \tag{3}$$

Let us assume that the Δt at the cluster head is dependent on the number of clusters/ groups in the network. So, the adaptive window length at the group level could be calculated as follows.

$$\Delta t = \left\lceil \left| \frac{-6.375n - 72}{4(|G| + \sigma - 2)} - 1 \right| \right\rceil \tag{4}$$

Figure 9 shows the affects of cluster size and window length on memory consumption at the sensor node and at the cluster head. Figures 9(a) and 9(b) shows that as the size of cluster decreases, the memory requirement at the sensor node and at the cluster head also decreases. Here, word *size* represents the number of nodes. Also, Figure 9(c) shows that the adaptive time window length is more efficient in terms of memory consumption as compared to the fixed time window length.

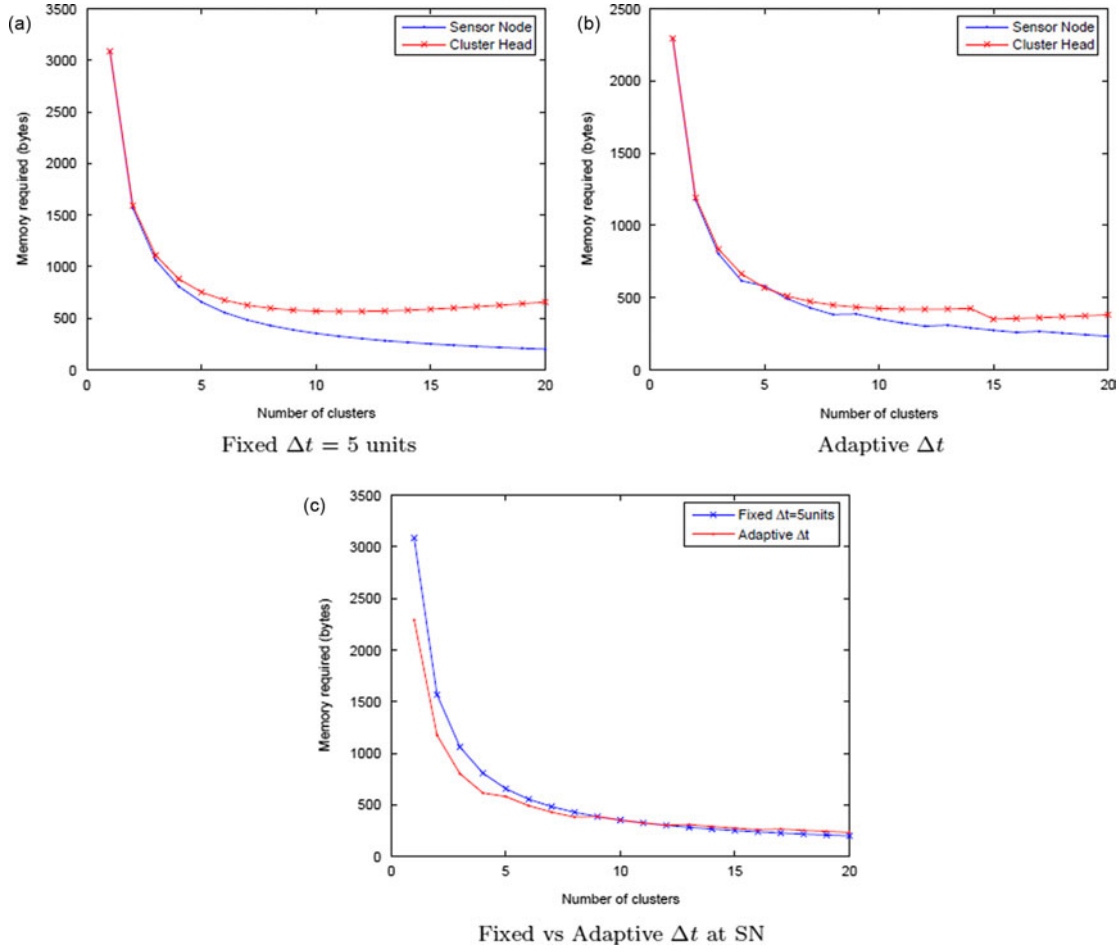


Figure 9. Memory Requirement of Complete Solution: $N = 100$.

4.2 Communication Overhead Analysis

Let us first assume a worst case scenario, in which every member node wants to communicate with every other node in the group and every group wants to communicate with the rest of the groups in the network. In order to calculate the trust value, assume that each node performs peer recommendation before start of any communication. Additionally, peer recommendation is performed in a secure manner. Let us assume that the network consists of |G| groups and the average size of groups is σ.

In the intra-group communication case, when node i wants to interact with the node j, node i will send maximum $\sigma - 2$ peer recommendation requests. In response of the peer recommendation request, node i will maximum receive $\sigma - 2$ responses. So, maximum communication overhead against one peer recommendation will be: $2(\sigma - 2)$. If node i wants to interact with all the nodes in the group, then the maximum communication overhead will be $2(\sigma - 1)(\sigma - 2)$. If all nodes want to communicate with each other, then the maximum communication overhead will be: $2\sigma(\sigma - 1)(\sigma - 2)$. Since peer recommendation is performed in a secure manner, therefore four additional control packets will be forwarded to generate session key. Therefore, the maximum intra-group communication overhead ($C_{\text{w-intra}}$) of the complete solution is:

$$C_{\text{w-intra}} = 4 \times 2\sigma(\sigma - 1)(\sigma - 2) = 8\sigma(\sigma - 1)(\sigma - 2) \tag{5}$$

In the inter-group communication case, when one group wants to interact with another group, it will send one peer recommendation request to the base station. Since cluster head already shared secret key with the base station, therefore the security component will not introduce any additional overhead. So, for each request the communication overhead is 2 packets. If group i want to communicate with all the groups then the maximum communication overhead will be $2(|G| - 1)$ packets. If all the groups want to communicate with each other, then the maximum inter-group communication overhead ($C_{\text{w-inter}}$) will be:

$$C_{\text{w-inter}} = 2|G|(|G| - 1) \tag{6}$$

Therefore, in the worst case, the maximum communication overhead C_{worst} introduce by the complete solution in the network is:

$$\begin{aligned} C_{\text{worst}} &= |G| \times C_{\text{w-intra}} + C_{\text{w-inter}} \\ C_{\text{worst}} &= |G| \times 8\sigma(\sigma - 1)(\sigma - 2) + 2|G|(|G| - 1) \\ C_{\text{worst}} &= |G| \times [8\sigma(\sigma - 1)(\sigma - 2) + 2(|G| - 1)] \end{aligned} \tag{7}$$

On average, communication overhead C_{avg} introduce by the complete solution in the network is:

$$\begin{aligned} C_{\text{avg}} &= \frac{|G| \times C_{\text{w-intra}}}{\sigma} + \frac{C_{\text{w-inter}}}{|G|} \\ C_{\text{avg}} &= \frac{|G| \times 8\sigma(\sigma - 1)(\sigma - 2)}{\sigma} + \frac{2|G|(|G| - 1)}{|G|} \\ C_{\text{avg}} &= 8|G|(\sigma - 1)(\sigma - 2) + 2(|G| - 1) \end{aligned} \tag{8}$$

In the best case, no peer recommendation will be performed by each node in the network. Nodes will take decision based on the direct observations. Before start of each session, four control packets are exchanged between communicating nodes.

At the network layer if r-IRL routing scheme (Shaikh et al., 2010) is used, then the communication overhead will increase with the factor of r. The summary of communication overhead for the two different cases is given in the Table IV. Figure 10 shows the comparison of the two possible combinations of the proposed solution.

Table IV. Communication Overhead of Complete Solution.

Cases	GTMS + LSec + IRL	GTMS + LSec + rIRL
Worst	$\|G\|[8\sigma(\sigma-1)(\sigma-2)+2(\|G\|-1)]$	$r\|G\| \times [8\sigma(\sigma-1)(\sigma-2)+2(\|G\|-1)]$
Average	$8\|G\|(\sigma-1)(\sigma-2)+2(\|G\|-1)$	$r[8\|G\|(\sigma-1)(\sigma-2)+2(\|G\|-1)]$

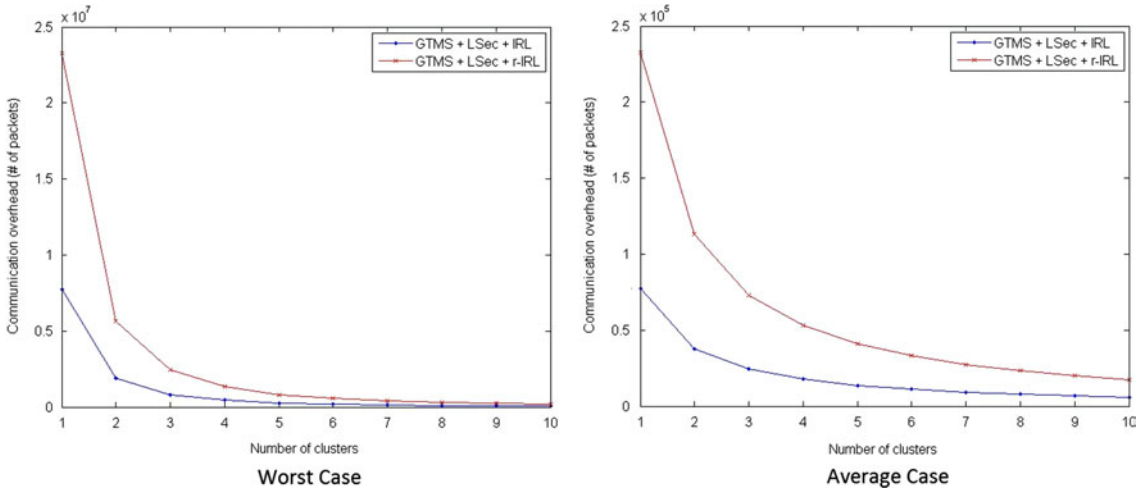


Figure 10. Communication Overhead of Complete Solution: $N = 100$, $r = 3$.

5. CONCLUSION AND FUTURE WORK

In the WSN domain, current research so far focuses on the privacy, security and trust components separately. However, efforts on developing integrated solution are lacking. In this work, the integrated privacy, security and trust solution for WSNs is presented that is needed for achieving completeness in the security solution. This paper describes the integration details of the privacy, security and trust components that are helpful in understanding the interactions between various components. This paper also provides theoretical analysis and evaluation of the complete solution from the perspective of memory consumption and communication overhead. Results show that the proposed solution is lightweight and suitable for large WSNs. In the future, we will implement the proposed solution in the simulator. That will provides more comprehensive results in terms of energy consumptions and communication overhead.

The security, privacy and trust concerns will exponentially increase when integrating WSN with cloud computing environment. In fact, recent researches (Ahmed & Gregory, 2011; Alamri et al., 2013; Zhu, Leung, Wang, Chen, & Liu, 2013) have been done on how to get benefit from the large scale resources that could be provided by the cloud. The huge amount of WSN data exchanged in such platform need to be secured and protected from any malicious attacks (including the cloud provider themselves). In the future, we would like to extend our proposed solution to sensor-clouds.

ACKNOWLEDGEMENTS

This research was supported by the MSIP (Ministry of Science, ICT & Future Planning), Korea, under the ITRC (Information Technology Research Center) support program supervised by the NIPA (National IT Industry Promotion Agency) (NIPA-2014-(H0301-14-1003)). This work was also supported by the Industrial Core Technology Development Program (100,49079, Development of Mining core technology exploiting personal big data) funded by the Ministry of Trade, Industry and Energy (MOTIE, Korea).

REFERENCES

Ahmed, K., & Gregory, M. (2011, December). Integrating wireless sensor networks with cloud computing. In *Proceedings of 7th IEEE international conference on mobile ad-hoc and sensor networks (MSN)* (pp. 364–366).

Ahmed, M., Huang, X., & Sharma, D. (2012). A novel misbehavior evaluation with dempster-shafer theory in wireless sensor networks. In *13th ACM International symposium on mobile ad hoc networking and computing* (pp. 259–260).

Aivaloglou, E., Gritzalis, S., & Skianis, C. (2007). Towards a flexible trust establishment framework for sensor networks. *Telecommunication Systems*, *35*, 207–213.

Alamri, A., Ansari, W. S., Hassan, M. M., Hossain, M. S., Alelaiwi, A., & Hossain, M. A. (2013). A survey on sensor-cloud: Architecture, applications, and approaches. *International Journal of Distributed Sensor Networks*, *2013*.

Boukerche, A., Xu, L., & El-Khatib, K. (2007). Trust-based security for wireless ad hoc and sensor networks. *Computer Communications*, *30*, 2413–2427.

Boyle, D., & Newe, T. (2008). Securing wireless sensor networks: security architectures. *Journal of Networks*, *3*, 65–77.

Chai, G., Xu, M., Xu, W., & Lin, Z. (2012). Enhancing sink-location privacy in wireless sensor networks through k-anonymity. *International Journal of Distributed Sensor Networks*, *2012*.

Chen, G., Branch, J., Pflug, M., Zhu, L., & Szymanski, B. (2005). SENSE: A wireless sensor network simulator. *Advances in Pervasive Computing and Networking*, 249–267.

Chen, H., & Lou, W. (2014). On protecting end-to-end location privacy against local eavesdropper in wireless sensor networks. *Pervasive and Mobile Computing*. http://dx.doi.org/10.1016/j.pmcj.2014.01.006. Published online 28 January 2014.

Cionca, V., Newe, T., & Dădârlat, V. T. (2012). Configuration tool for a wireless sensor network integrated security framework. *Journal of Network and Systems Management*, *20*, 417–452.

Duan, J., Yang, D., Zhu, H., Zhang, S., & Zhao, J. (2014). TSRF: A trust-aware secure routing framework in wireless sensor networks. *International Journal of Distributed Sensor Networks*, *2014*.

Feng, R., Che, S., Wang, X., & Yu, N. (2013). Trust management scheme based on D-S evidence theory for wireless sensor networks. *International Journal of Distributed Sensor Networks*, *2013*, 1–9.

Ganeriwal, S., Balzano, L. K., & Srivastava, M. B. (2008). Reputation-based framework for high integrity sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, *4*, 15–37.

Gong, Z., Hartel, P., Nikova, S., Tang, S. H., & Zhu, B. (2014). TuLP: A family of lightweight message authentication codes for body sensor networks. *Journal of Computer Science and Technology*, *29*, 53–68.

Gómez Mármol, F., & Martínez Pérez, G. (2011). Providing trust in wireless sensor networks using a bio-inspired technique. *Telecommunication Systems*, *46*, 163–180.

Haowen Chan, A., & Perrig, A. (2003). Security and privacy in sensor networks. *Computer*, *36*, 103–105.

Healy, M., Newe, T., & Lewis, E. (2008). Analysis of hardware encryption versus software encryption on wireless sensor network motes. *Smart Sensors and Sensing Technology, Lecture Notes in Electrical Engineering*, *20*, 3–14.

Hsu, S. J., Chen, C. H., Chen, S. H., Huang, W. T., Chang, Y. J., & Chen, Y. Y. (2010). Conserving bandwidth in a wireless sensor network for telemedicine application. *Intelligent Automation & Soft Computing*, *16*, 537–551.

Huang, S. I., Shieh, S., & Tygar, J. D. (2010). Secure encrypted-data aggregation for wireless sensor networks. *Wireless Networks*, *16*, 915–927.

Ishmanov, F., Kim, S. W., & Nam, S. Y. (2014). A secure trust establishment scheme for wireless sensor networks. *Sensors*, *14*, 1877–1897.

Jian, Y., Chen, S., Zhang, Z., & Zhang, L. (2007). Protecting receiver-location privacy in wireless sensor networks. In *INFOCOM 2007. 26th IEEE international conference on computer communications* (pp. 1955–1963).

Jose, J., & Princy, M. (2013, March). PEPPDA: Power efficient privacy preserving data aggregation for wireless sensor networks. In *Proceedings of 2013 international conference on emerging trends in computing, communication and nanotechnology* (pp. 330–336).

Kamat, P., Zhang, Y., Trappe, W., & Ozturk, C. (2005). Enhancing source-location privacy in sensor network routing. In *Proceedings of the 25th IEEE international conference on distributed computing systems (ICDCS 2005)* (pp. 599–608).

Kambourakis, G., Gritzalis, S., & Park, J. H. (2010). Device authentication in wireless and pervasive environments. *Intelligent Automation & Soft Computing*, *16*, 399–418.

Karlof, C., Sastry, N., & Wagner, D. (2004). TinySec: a link layer security architecture for wireless sensor networks. In *Proceedings of the 2nd International Conference on Embedded networked sensor systems* (pp. 162–175).

Li, X., Zhou, F., & Du, J. (2013). LDTS: A lightweight and dependable trust system for clustered wireless sensor networks. *IEEE Transactions on Information Forensics and Security*, *8*, 924–935.

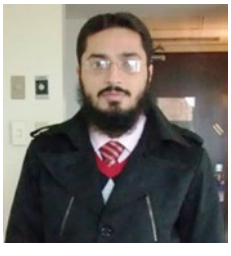
Li, Y., Li, J., Ren, J., & Wu, J. (2012). Providing hop-by-hop authentication and source privacy in wireless sensor networks. In *IEEE international conference on computer communications* (pp. 3071–3075).

Li, Y., & Ren, J. (2010, March). Source-location privacy through dynamic routing in wireless sensor networks. In *INFOCOM, 2010 Proceedings IEEE* (pp. 1–9).

Liu, K., Abu-Ghazaleh, N., & Kang, K. (2007). Location verification and trust management for resilient geographic routing. *Journal of Parallel and Distributed Computing*, *67*, 215–228.

Mainwaring, A., Culler, D., Polastre, J., Szewczyk, R., & Anderson, J. (2002). Wireless sensor networks for habitat monitoring. In *Proceedings of the 1st ACM international workshop on wireless sensor networks and applications* (pp. 88–97).
Misra, S., & Xue, G. (2006). Efficient anonymity schemes for clustered wireless sensor networks. *International Journal of Sensor Networks*, *1*, 50–63.
Nguyen, S. T., Cayirci, E., & Rong, C. (2014). A secure many-to-many routing protocol for wireless sensor and actuator networks. *Security and Communication Networks*, *7*, 88–98.
Oliveira, L. B., Aranha, D. F., Gouvêa, C. P., Scott, M., Câmara, D. F., López, J., & Dahab, R. (2011). TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks. *Computer Communications*, *34*, 485–493.
Ozturk, C., Zhang, Y., & Trappe, W. (2004). Source-location privacy in energy-constrained sensor network routing. In *Proceedings of the 2nd ACM workshop on security of ad hoc and sensor networks* (pp. 88–93).
Park, T., & Shin, K. G. (2004). LiSP: A lightweight security protocol for wireless sensor networks. *ACM Transactions on Embedded Computing Systems*, *3*, 634–660.
Perrig, A., Stankovic, J., & Wagner, D. (2004). Security in wireless sensor networks. *Communications of the ACM*, *47*, 53–57.
Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., & Culler, D. E. (2002). SPINS: security protocols for sensor networks. *Wireless Networks*, *8*, 521–534.
Shaikh, R. A., Jameel, H., D'auriol, B. J., Lee, H., Lee, S., & Song, Y. (2010). Achieving network level privacy in wireless sensor networks. *Sensors*, *10*, 1447–1472.
Shaikh, R., Jameel, H., d'Auriol, B., Heejo Lee, H., Sungyoung Lee, S., & Young-Jae Song, Y. (2009). Group-based trust management scheme for clustered wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, *20*, 1698–1712.
Shaikh, R., Lee, S., Khan, M., & Song, Y. (2006). LSec: Lightweight security protocol for distributed wireless sensor network. In *Personal wireless communications* (pp. 367–377).
Syed, M. K. R., Lee, H., Lee, S., & Lee, Y. K. (2010). MUQAMI+: A scalable and locally distributed key management scheme for clustered sensor networks. *Annals of Telecommunications – Annales des Télécommunications*, *65*, 101–116.
Tan, G., Li, W., & Song, J. (2014). Enhancing source location privacy in energy-constrained wireless sensor networks. In *Proceedings of international conference on computer science and information technology* (pp. 279–289).
Wood, A. D., Fang, L., Stankovic, J. A., & He, T. (2006). SIGF: A family of configurable, secure routing protocols for wireless sensor networks. In *Proceedings of the 4th ACM workshop on security of ad hoc and sensor networks* (pp. 35–48).
Yang, J., & Jung, S. H. (2010). The case study of system architecture in wireless sensor networks: The kindergarten safety system (KSS). *Intelligent Automation & Soft Computing*, *16*, 507–517.
Yao, Z., Kim, D., & Doh, Y. (2006). PLUS: Parameterized and localized trust management scheme for sensor networks security. In *Proceedings of the 3rd IEEE international conference on mobile ad-hoc and sensor systems* (pp. 437–446).
Yu, Y., Li, K., Zhou, W., & Li, P. (2012). Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures. *Journal of Network and Computer Applications*, *35*, 867–880.
Zhang, J., Shankaran, R., Orgun, M. A., Varadharajan, V., & Sattar, A. (2010). A trust management architecture for hierarchical wireless sensor networks. In *Proceedings of IEEE 35th conference on local computer networks (LCN)* (pp. 264–267).
Zhu, C., Leung, V., Wang, H., Chen, W., & Liu, X. (2013, December). Providing desirable data to users when integrating wireless sensor networks with mobile cloud. In *IEEE 5th international conference on cloud computing technology and science (CloudCom)* (Vol. 1, pp. 607–614).
Zhu, S., Setia, S., & Jajodia, S. (2006). LEAP +: Efficient security mechanisms for large-scale distributed sensor networks. *ACM Transactions on Sensor Networks*, *2*, 500–528.

NOTES ON CONTRIBUTORS



Riaz Ahmed Shaikh received Ph.D. degree from Computer Engineering Dept., of Kyung Hee University, Korea, 2009. He is an assistant professor at the Computer Science Dept. of the King Abdulaziz University, Jeddah, Saudi Arabia since 2012. His research interest includes privacy, security, trust management, WSNs, and vehicular networks.

Sungyoung Lee received M.S. and Ph.D. degrees in Computer Science from Illinois Institute of Technology, Chicago, USA in 1987 and 1991 respectively. He has been a professor in the Computer Engineering Department of Kyung Hee University, Korea since 1993. His current research focuses on Ubiquitous Computing and Applications, WSNs, Real-time Systems and Embedded Systems.

Aiid Albeshri received M.S. and Ph.D. degrees in Information Technology from Queensland University of Technology, Brisbane, Australia in 2007 and 2013 respectively. He has been an assistant professor at the Computer Science Department of the King Abdulaziz University, Jeddah, Saudi Arabia since 2013. His current research focuses on Security and Trust in Cloud computing.