Applied Mathematics & Information Sciences Letters
An International Journal

http://dx.doi.org/10.18576/amisl/060206

Analyses of Security Protocols in Wireless Sensor Network Using Model Checking

Zeinab Varaminy Bahnemiry

Department of Computer Engineering, Mazandaran University of Science & Technology, Iran

Received: 28 Apr. 2017, Revised: 24 Dec. 2017, Accepted: 27 Dec. 2017
Published online: 1 May 2018

Abstract: In this paper, a formal survey in security protocols of wireless sensor networks is investigated. These protocols include TinySec, LEAP, TinyPK, MiniSec, SNEP and Tesla. These protocols are modeled by High Level formal language and also by model Checking tool known as AVISPA (Automated Validation of Internet Security Protocol an Application) is verified. Each of these protocols supports security properties such as authenticity, confidentiality, broadcast protection and refreshment messages. In surveys A or several security property is investigated. As a result, two attacks have been found. According to this result indicate the protocol is safe or not [1,2,3].

Keywords: Sensor Wireless, Model checking, security protocol, AVISPA Tool

1 Introduction

Today, due to many application wireless sensor networks, the topic of security in wireless sensor networks is a big challenge. Due to low capabilities of devices, high energy consumption and the lower computational power, using traditional security protocols is very difficult. There are two big problems in security protocols. First, the overload in transition of messages that creating high energy consumption should be reduced at a minimum cost. Second, low computational power shows that in this case should be used special cryptographic algorithms with less powerful processors [1,2,3]. As a result, for solving these problems we should consider new approaches. In secure networks, several properties should be considered: Key establishment, secrecy, trust setup, privacy and authentication. For exchanging messages, the nodes require the secure and efficient Key distribution. So, it is necessary to survey secure protocols. TinySec Protocol, which is used for authentication and encryption and has link layer security architecture. LEAP is another protocol which is used for authentication and localized encryption that base on key management. This protocol supports four kinds of keys. TinyPK protocol, is based on key management [1]. MiniSec protocol is a secure protocol in network [2]. In this protocol, Confidentiality, authentication, broadcast protection and refreshment messages are supported with low energy consumption. SNEP protocol (Sensor Network Encryption Protocol) is the main base for data confidentiality, two-party data authentication, replay protection and weak message freshness in wireless sensor network [3]. μ Tesla, based on asymmetric cryptography for providing broadcast authentication that is a main security service in distributed sensor networks [5]. This protocol is one of the technics in Model checking and work base on formal method and also is simulated in different tools. One of the advantages is automation. Also, in this technique determines that the system work base on our expectation or not. In case of lack of good performance is pursued defect of the system.

There are different tools for model checking such as: Spin, UPPAAL, Murφ. It is better to use a special purpose model checking tool that is suitable for verifying security protocols. One of these tools is AVISPA that use from a high-level formal language (HLPSL). AVISPA, after determining model of the system, translates it into an intermediate format [1,2,3]. This paper is organized as follows. In Section 2 a brief overview of TinySec, LEAP, TinyPK, MiniSec, SNEP and μ Tesla is given. Architecture of model checking tools is presented in section 3. In section 4, the results of analysis protocols by AVISPA are investigated and in each protocol some different cases are considered. After that in section 5,

* Corresponding author e-mail: varamini.z@gmail.com

μ Tesla protocol is investigated. Finally, conclusion and future works are presented.

2 Introduction to Protocols

TinySec: a security architecture is implemented as a link layer and cost overhead is less than 10 percent. This protocol is used as a standard library in TinyOs [6]. The main goal of this protocol is security, access control, message authenticity and integrity and confidentiality. This protocol in application layer has two operations: authentication and secure encryption. Packets are authenticated by CBC-MAC Message Authentication Code and secure encryption is done with an initialization vector of 8 Byte and used from CBC (cipher block chaining). As a result, by using these two operations, there are two packets. TinySec-AE, which is presented for authentication and encryption messages and TinySec-Auth, which is presented for authentication messages. These two packets are shown in figure 1.

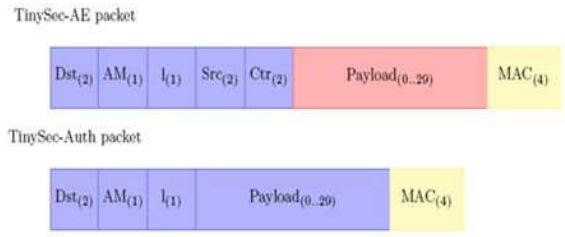

Fig. 1: TinySec packet formats: TinySec-AE and TinySec-Auth [1]

Shared keys are used for encryption and decryption data. TinySec could be combined with any keying mechanism. As a result, Localized Encryption and Authentication Protocol and TinyPK as a keying mechanism has been used. LEAP: LEAP creates 4 kinds of keys for each sensor node. The base station is shared with an individual key, another sensor node is shared with a pairwise key, multiple neighboring nodes is shared by a cluster key, and a group key that is shared by all the nodes in the network. LEAP keying mechanisms are shown in figure 2 [1].

TinyPK: TinyPK supports confidentiality and authentication for wireless sensor networks. In this protocol a third party is authenticated using the means of sensor motes and asymmetric keys. A small public key is needed. Protocol operation is divided with two steps: the external party authentication and the node authentication. Firstly, the external party authenticates itself. Secondly, the node and the external party are shared with the network key. Furthermore, Diffie-Hellman exchange is used for creating create a new key pair. Each node has a

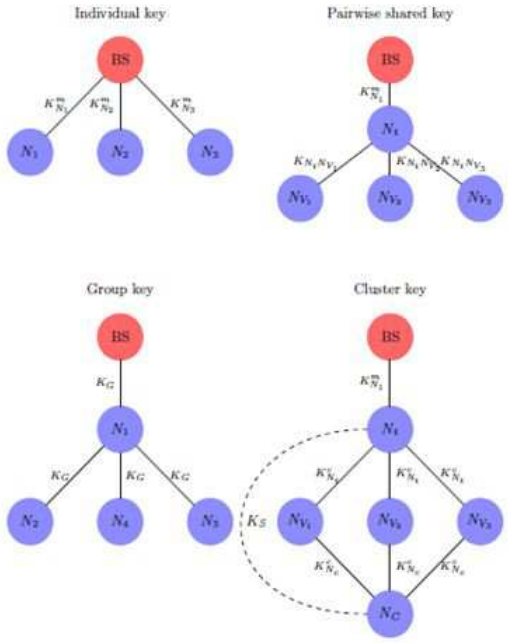

Fig. 2: LEAP keying mechanisms [1]

static Diffie-Hellman key, while an ephemeral Diffie-Hellman key is produced by the third party [2].

MiniSec: for achieving better energy needs, it works in two modes: unicast packets MiniSec-U, and broadcast packets. At MiniSec-U, the message between two nodes A and B is protected. Each pairwise of nodes shares asymmetric key pair for encryption between A and B. At MiniSec-B, the encryption is used and two ways are used for defense against broadcast attacks. Shared keys are used for encryption and decryption and MiniSec protocol uses LEAP mechanism. MiniSec as a secure protocol offers data using coded block mode, encryption mode and authentication and also confidentiality. In MiniSec protocol key distribution or computational algorithm is not addressed, but LEAP is proposed as a solution of key management [3].

SNEP: As basic primitives offer confidentiality, authentication between two nodes, data integrity and weak message freshness in a wireless sensor network. This protocol is modeled at two scenarios. The first model is communication between the base station and network nodes is to get node confidential information. The second model is a key distribution protocol in a sensor network. In this protocol is used for shared counter. A Message Authentication Code (MAC) is used in each message and achieve by CBC-MAC algorithm over the ciphered data. CBC-MAC algorithms encrypt a message M in CBC mode with a symmetric key and zero initialization vector [4]. The protocols and their security properties have been classified in Table 1.

Table 1: Classification of the Wireless Sensor Network Protocols and the Security Properties

Protocols / Security Properties	TinySec	TinyPK	MiniSec	SNEP	ZigBee
Access Control	√				
Message Integrity	√			√	√
Weak Message Freshness			√	√	
Protection Against Replay Attacks	√		√		√
Authentication		√	√		
Confidentiality	√	√	√	√	√

3 Architecture of Model Checking tool for Analysis of Security Protocols AVISPA

This tool for determining protocol and their property uses from high level formal language.

The architecture of this tool is shown in figure 3.

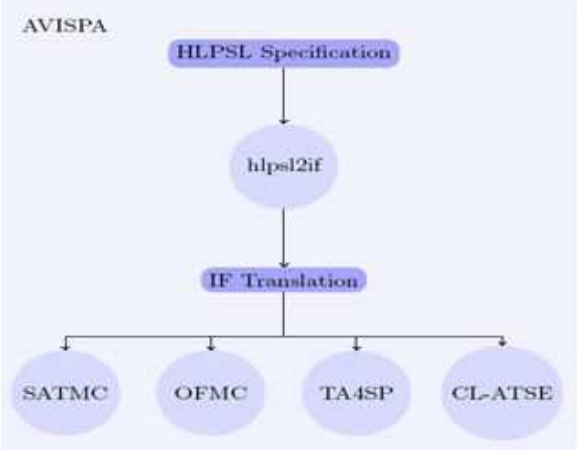

Fig. 3: Architecture of AVISPA Tool [4]

After determining system model, AVISPA translate it to intermediate model. Intermediate section is used as entries for 4 last sections. These sections are included: SATMC, OFMC, CL-ATSE and TA4SP.

Security Protocol Specifications in SATMC are translated automatically into propositional logic, which can find attacks in protocols. At OFMC, two ideas are combined for analyzing security protocols. The first idea is the use of lazy data types for analyzing security protocols. At second idea, for modeling a lazy Dolev-Yao is used for the integration of symbolic techniques and optimizations. At Constraint Logic (CL-Atse), has implemented the deduction rules. These rules allow anyone to against a generic intruder automatically a protocol execute. At TA4SP is rewriten the regular tree languages [4].

There are two kinds of roles at Avispa: basic roles and composed roles. A protocol participant initial knowledge, the initial state and a set of transitions, which describes the behavior of the participant, is shown at a basic role. The basic roles are combined to describe protocol sessions that are combined roles. For describing the protocols and the models at Avispa, is used common notation [4].

4 Protocols Analysis with AVISPA Tool

Often at these protocols is not used special mechanism for keying, but in this paper is used for LEAP keying mechanism. So, at analyses has used the combination of each protocol with this mechanism.

4.1 Analysis of LEAP, TinySec and TinyPK Protocols

The combination of LEAP and TinySec protocol, or TinySec and TinyPK presents completed solution. LEAP, or TinyPK is responsible for shared keys and TinySec is responsible for authentication and encryption the messages that are exchanged between nodes. As a result, there are 6 kinds of configuration with these 3 protocols that depends on keying mechanism and situation of nodes that are connected together. In all cases, main key inside each node is saved on the network. Any messages into the radio communication channel are injected by an intruder. First case: In this case a base node sends a request for a normal node, which a unique key is shared with the base station. In this case of the message is used from TinySec-AE packets (figure 4).

The properties we have to analyze are the following:

–Authentication of Data1 and Data2, the node Ni and the base station (BS) share the same value for Data1 and Data2 and both execute the same session of the protocol. So, the bilateral authentication is proved and

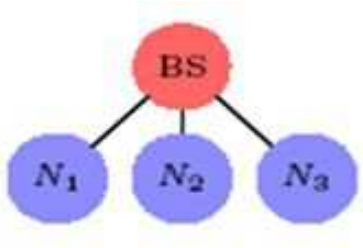

Fig. 4: Sensor network: first cases and second case [2]

the integrity of the message is guaranteed.

–Confidentiality of Data1 and Data2, Data1 and Data2 are secret values shared between Ni and Base Station, and they are not known by an intruder or third parties.

Result of Analysis by AVISPA: In TinySec protocol, broadcast attack is not managed but this protocol is secure even if a node is attacked by an intruder.

Second Case: A base node sends a request for a normal node from the unique key by TinySec-Auth messages instead of TinySec-AE messages. In this case, confidentiality mechanism is not supported. So, only authentication is supported. The bilateral authentication between the Base Station and Ni, by means of the MAC messages, and the integrity of messages is proved. There is a replay attack that is omitted.

Third Case: A node shares a pairwise key with each of its immediate neighbors (figure 5).

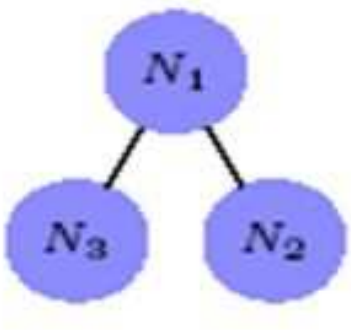

Fig. 5: Sensor network: third case and fourth case [2]

The properties we have to analyze are the following:

–Authentication of Data A and Data B, Nodes A and B share the same value and both execute the same session of the protocol.

–Confidentiality of Data B, Data B is a secret value that is shared between A and B, and is unknown to an intruder or third parties.

Result of Analysis by AVISPA: In this case AVISPA has an attack. Node A and Node B are communicating with the intruder.

Fourth Case: A node shares a cluster key with each of its immediate neighbors.

The properties we have to analyze are the following:

–Authentication of KC, Data A and Data B, nodes A and B share the same value for KC, Data A and Data B and both execute the same session of the protocol.

–Confidentiality of Data B and KC, Data B and KC are secret values that are shared between A and B, and they are unknown to an intruder or third parties.

Result of Analysis by AVISPA: After analyzing, an attack is found.

Fifth Case: A node shares a cluster key with non-immediate neighboring nodes (figure 6).

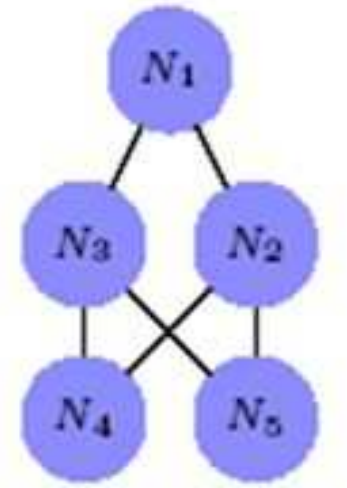

Fig. 6: Sensor Network: fifth case [2]

Result of Analysis by AVISPA: only has a replay attack that is not important. So, this protocol is secure [1,2].

Sixth Case: a third party establishes an authenticated communication channel with a sensor network by TinyPK. In this case, it has an attack and the sensor node should detect that messages are replayed. Thus, this attack is not important and the protocol is secure [3].

4.2 Analysis of MiniSec Protocol

At figure 7, two cases at network configuration is considered: MiniSec-U and MiniSec-B. Connection or

disconnection the nodes to the network are not dynamic. So, the analysis is simplified.

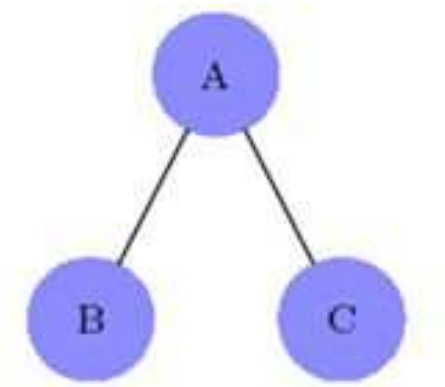

Fig. 7: Sensor network for the two analyzed cases at MiniSec [3]

4.2.1 MiniSec-U

In this case, a node A sends a request to its neighbor nodes B and C.

The properties we have to analyze are the following:

–Authentication, the node A and the node B share the same value for H3, H3, P4 and the same session of the protocol is executed on all of them. So, there are not replayed attacks and the freshness of messages is guaranteed.

–Confidentiality, secret values that shared between A and B, and they are unknown by an intruder or third parties.

In this case, there is a sender node A and two receiver nodes B and C. Also, there is not an attack.

4.2.2 MiniSec-B

A node A create a cluster key among the network nodes and it broadcasts a message. The cluster key is encrypted by the shared key of the node A and its neighbor. For updating node configuration or internal data, broadcast messages are used. So, the node A does not expect an answer to its broadcast message.

The properties we have to analyze are the following:

–Authentication, the node A and the node B and the node C share the same value for $H1$ and $P1$ and all of them execute the same session of the protocol. In this case, there are not replayed attacks and the freshness of messages is guaranteed.

–Confidentiality, a secret value shared between A, B and C, and they are unknown by an intruder or third parties [3].

4.3 Analysis of SNEP Protocol

This protocol is modeled at two models:

BS-N: Request from the base node to a normal node.

N-N: Key distribution between two nodes.

In figure 8, the base station is the main way for nodes to communicate with the outside world. So, compromising the whole network means compromising the base station. Thus, the base station is a trusted component and cannot be impersonated. The network is in a stable phase

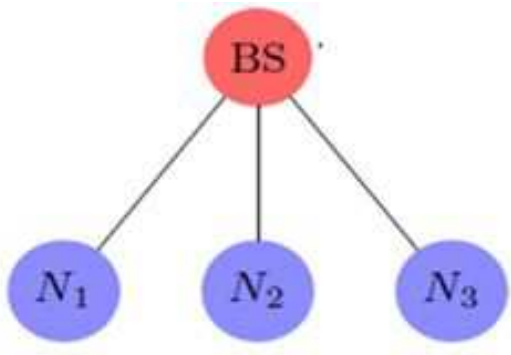

Fig. 8: Sensor network for two classes at SNEP [4]

Now, we evaluate these two models.

Case Base Station→ Node: our analyses a request from the base station to the nodes.

The properties we have to analyze are the following:

–Authentication, the node Ni and the base station BS share the same value for exchange messages and both execute the same session of the protocol. Bilateral authentication is proved and the integrity of the message is guaranteed.

–Confidentiality, there is a secret value that shared between Ni and Base Station and they are unknown by an intruder or third parties.

Result of Analysis by AVISPA: the first message is not secured, there is an attack. The intruder sends a false request for a node. There is not any authentication information in this message.

Thus, the node thinks that the base station sent the message, it responses the request. Because intruder has not the value of Km, the intruder cannot understand the value of Message2. But, the intruder consumes resources

Table 2: Results of Analysis Security Protocols By Model Checking AVISPA

Protocols	Cases	Key Type	Authentication	Confidentiality	Message Freshness	Integrity	Message Authenticity	Attack Detection	Secure Protocol
TinySec TinyPK LEAP	First case: Sharing Base Node to Normal Node	Unique Key	Message Authentication Code	√		√	√		√
	Second case: Sharing Base Node to Normal Node	Unique Key	Message Authentication Code			√	√	√	√
	Third Case: Sharing Base Node to Immediate Neighbors	Pairwise key	√	√				√	
	Fourth Case: Sharing Base Node to Immediate Neighbors	Cluster Key	√	√				√	
	Fifth Case: Sharing Base Node to non-immediate neighboring nodes	Cluster Key						√	√
	Sixth Case: Sharing Base Node to Third Party	Asymmetric key TinyPK	√				√	√	√
MiniSec	First Case:MiniSec (MiniSec-U)	Shared Key	√	√	√				√
	Second Case:MiniSec (MiniSec-B)	Cluster Key	√	√	√				√
SNEP	First Case: (N-BS)	Shared Key	Message Authentication Code	√	√	√	√	√	√
	second Case: (N-N)	Shared symmetric key	√	√	√				√

and bandwidth. For preventing, we can compute a MAC over the first message.

Case Node→ Node: By asymmetric key protocols at key distribution, we could exchange a shared symmetric key but resource consumption is not feasible. So, symmetric key algorithms are used. SNEP has a key distribution solution based on the base station. The node A shares a key with the node B.

The properties we have to analyze are the following:

–Authentication of NA and NB, the node A, the node B and the base station BS share the same value for NA and NB and the same session of the protocol is executed by them. There are not replayed attacks and the freshness of messages is guaranteed.

–Authentication of shares key SKab, the node A, the node B and the base station BS share the same value for NA, NB and SKab and the same session of the protocol is executed by them. A bilateral

authentication is proved between node A and node B through the base station BS because they share the same key SKab.

–Authentication of Msg1 and Msg2, i.e., the node A and the node B share the same value for Msg1 and Msg2 and the same session of the protocol are executed by them. The bilateral authentication is proved by the MAC, and the integrity of the message is guaranteed.

–Confidentiality of Msg2, Msg2 is a secret value that is shared between A and B, and they are unknown by an intruder or third parties.

–Confidentiality SKab, SKab is a secret value that is shared among A, B and BS, and they are unknown by an intruder or third parties.

Result of Analysis by AVISPA: In this case, any attack is not detected [4].

The results of the analysis the protocols by AVISPA are shown that the protocols often are secure. In fact, there are replay attacks and we could not consider them. As a result, these are presented in Table 2.

5 Analysis of μTesla Protocol

The main idea in this protocol is asymmetric cryptographic mechanisms through a delayed disclosure of symmetric keys. In this case, sender broadcasts the message that creates with a secret key to the nodes. After a time, the secret key is disclosed. Until disclosure, the receiver buffer the packets. Then, is authenticated the packets. The limitation of Tesla is that the initial information should arrive to each node before authentication of the message [7].

μTesla is consist of three steps: 1- Sender setup: The sender generates a keychain and the last key chooses key chain and other keys are computed with this key. 2- Broadcasting authenticated packets: Time is divided into time intervals and each key of the key chain are associated with one time interval. 3- Authenticating broadcast packets: When a node receives the packets, it should ensure that the packet could not have been spoofed by an adversary. Then, the sender and receivers should synchronize loosely [8]. After the end of the time interval and disclosure of key value after delayed time, the receiver could authenticate the packet [10].

At μTesla freshness of messages is guaranteed [8]. Also, integrity and Communication Authenticity is guaranteed [9]. This protocol at two attacks DOS: Danial of Service and Wormhole is vulnerable. Liu and Ning improve Tesla. They used multicasting instead of Unicasting key chain. A series of schemes with a Predetermination of key chains was presented and finally multi-level key chain technique was presented. As a result, μTesla is resistant to denial of service attacks [5].

6 Conclusion and Future Works

In this paper, a formal approach for analyzing security in wireless sensor networks by AVISPA is presented. At different protocols investigated different security properties and by investigating AVISPA we get results of attacks at protocols.

Several models for networks are presented by considering node situations. TinySec protocol is used for authentication and encryption. LEAP is used for Key distribution mechanism. At TinyPK, a third party is authenticated using the means of sensor motes and asymmetric keys. There are two cases for MiniSec protocol. In the first case, connotation at the nodes is investigated by MiniSec-U and there is a secure network. So, there are not any attacks. In the second case, MiniSec-B is investigated. In this case, the message is released with a secure way at the network. Also, there are not any attacks. Two models at SNEP is investigated. By evaluating first model, detecting an attack. So, SNEP protocol supports refreshment messages, authenticity, integrity and encryption.

Future works are developing the analysis about other security protocols in wireless sensor network such as ZigBee and survey LEAP for security properties exactly. Also, a new model intruder and new model checking will be presented.

References

[1] Llanos Tobarra, Diego Cazorla, Fernando Cuartero, Gregorio Daz, and Emilia Cambronero, Model Checking Wireless Sensor Network Security Protocols: TinySec + LEAP, Springer, 2007.
[2] Llanos Tobarra, Diego Cazorla, Fernando Cuartero, Gregorio Daz, and Emilia Cambronero, Model Checking Wireless Sensor Network Security Protocols: TinySec + LEAP+TinyPK, Springer, 2007.
[3] Llanos Tobarra, Diego Cazorla, Fernando Cuartero, and Gregorio Diaz, Analysis of security protocol MiniSec for Wireless Sensor Networks, Springer 2007.
[4] LLANOS TOBARRA, DIEGO CAZORIA, FERNANDO CUARTERO, SECURITY IN WIRELESS SENSOR NETWORKS: A FORMAL APPROACH , Springer, 2006.
[5] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary, Wireless Sensor Network Security: A Survey, Security in Distributed, Grid, and Pervasive Computing Yang Xiao, (Eds.), 2006 Auerbach Publications, CRC Press.
[6] Eric Platon and Yuichi Sei, Security Software Engineering in Wireless Sensor Networks, Progress in Informatics, No5, Page 49-6, March 2008.
[7] Adrian Perrig, Robert Szewczyk, J.D.Tygar, Victor Wen and David E. Culler, SPINS: Security Protocols for Sensor Networks, Wireless Networks 8,521-534,2022,2002 Kluwer Academic Publishers. Manufactured in the Netherlands.
[8] Llanos Tobarra, Diego Cazorla, Fernando Cuartero and J. Jose Pardo; Modelling Secure Wireless Sensor Networks

Routing Protocols with Timed Automata , ACM 978-1-60558-239, October 31, 2008, Vancouver, BC, Canada.
[9] Hao Chen; Efficient Compromising Resilient Authentication Schemes for Large Scale Wireless Sensor Networks ; ACM 978-1-60558-923-7/10/03; March 22-24, 2010, Hoboken, New Jersey, USA.
[10] Kun-Won Jang, Woo-sik Jung, Dong-kyu Shin and Moon-Seog Jun; Design of Secure Clustering Routing Protocol uses SNEP and TESLA on Sensor Network Communication; IJCSNS International Journal of Computer Science and 172 Network Security, VOL.6 No.1B, January 2006.

Zeinab Varaminy Bahnemiry received the Master degree in Department of Computer Engineering at Mazandaran University of Science & Technology in Iran. Her research interests are in the areas of Knowledge Discovery and Intelligent Systems, network, information systems.