International Journal of Systems Signal Control and Engineering Application 10 (1-6): 48-60, 2017
ISSN: 1997-5422

PKI Session Key Distribution in WSN Using Fuzzy Rule Based System

[1]Y.M. Wazery and [2]Mohamed Abd-ELfattah
[1]Department of Information System, Faculty of Computers and Information,
Minia University, Minia, Egypt
[2]Department of Information System,
Faculty of Computers and Information, Benha University, Benha, Egypt

Abstract: Wireless Sensor Network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions. WSN is a gateway that provides wireless connectivity back to the wired world or the distribution contract system includes. The nature of WSN as it is distributed and located in extreme conditions poses many security challenges to this type of networks. Ensuring security in WSN is challenging because most devices are resource constrained. In addition, different protocols that are used in these networks use their own set of security requirements. In this study, the security requirements of WSN are firstly identified. Then Public Key Infrastructure (PKI) is pointed out to be a feasible solution for distributing session keys, it has some difficulties to satisfy the requirements in availability, privacy preservation and scalability. PKI could be used in authenticating units and session keys. To complement the functions of PKI and overcome the rapidly changing conditions fuzzy rule based systems is used to provide a very convincing solution to decide the accurate session key length and other factors in WSN.

Key words: WSN, security, wireless, communication, fuzzy, PKI, KNN

INTRODUCTION

WSN plays an important role in modern communication technology. WSNs are a kind of MANETs that comprise of a vast number of asset obliged sensor units. The adaptability in arrangement furthermore, support advances WSN's applications in many fields including military, observing natural phenomena, open field security checking, crisis and emergency management. For instance, WSNs can be utilized to distinguish and track the interruption of adversary's tanks or units in a combat zone to screen ecological contaminations or to measure activity streams in a movement arrange. However, the characteristics of the wireless sensor network make the incorporating security very challenge. The constraints on sensor make the design and operation exceedingly different from the contemporary wireless networks. The existing security mechanisms for the wire-line and wireless networks cannot apply to the wireless sensor network because of the constrained energy, memory and computation capability. Thus, resource conscious security protocols and management techniques become necessity (Feng *et al*., 2015a, b).

Due to its nature and reason for deploying WSNs come with physical, security, node and network limitations making them more complicated those limitations could be seen as follows (Feng *et al*., 2015a, b).

Node limitations: A typical sensor node has a relatively small processing capabilities (4-8 MHz), having a small RAM measured in Kilobytes, 128 KB flash and ideally 916 MHz of radio frequency. Heterogeneous nature of sensor nodes is an additional imitation which prevents one security solution. Due to the deployment nature, sensor nodes would be deployed in environments where they would be highly prone to physical vandalism.

Security limitations: The main concern in this research is about security issues in WSN. Sensor systems are frequently utilized as a part of mission critical situations, for example, in military and social insurance applications. As comprehended, these situations have requesting security prerequisites that must be tended to at the underlying period of plan. Various security issues exist in WSN and should be investigated in detail so as to configure suitable security instruments and beat security issues that emerge in the sensor environment. Nonetheless, planning new security conventions and components is compelled by the capacities of the sensor entities and nodes.

Corresponding Author: Y.M. Wazery, Department of Information System, Faculty of Computers and Information, Minia University, Minia, Egypt

Network limitations: Sensor networks suffer from some network limitations where they don't have a stable physical and they are based on insecure wireless media.

Physical limitations: Sensor systems organization naturally outdoor in the open and threatening situations in numerous applications makes them profoundly defenseless against catch and vandalism. Physical security of sensor units with sealed material increases the sensor unit cost.

Security is a standout amongst the most essential issues in WSNs principally in light of the fact that WSNs are typically sent in antagonistic or remote situations and work in an unattended way (Elmazi *et al*., 2016).

Threats to sensor networks can be either application-dependent or application-independent. Attacks in the former category target specific network functionalities such as routing (Karlof and Wagner, 2003; Hanafy *et al*., 2012), node localization (Poovendran *et al*., 2007; Sun *et al*., 2007; Hanafy *et al*., 2013; Inaba *et al*., 2015), time synchronization (Radha *et al*., 2007; Hanafy *et al*., 2012), data aggregation (Sun *et al*., 2007; He *et al*., 2007; Inaba *et al*., 2015; Kulla *et al*., 2014) and so on while attacks in the latter category affect a wide variety of applications from object tracking and fire alarming to battlefield surveillance. Until recently, research on intrusion detection in WSNs has focused on the former category (see a recent survey (Sun *et al*., 2007) for an example where application-independent detection is completely absent) (Karlof and Wagner, 2003).

The use of PKI in WSN environments provides more strength to the security in WSN, the session key is to be treated and ciphered through a two non-related keys that makes it harder to track any of them.

In order to keep track with the extendable and rapidly changing nature of WSN, it is suitable to use fuzzy decision making scheme which will be capable of tracking the sudden changes in the parameters given to the security system.

Literature review

Public Key Infrastructure (PKI): Communication is the key factor in the modern era industry. One of the most important factors in communication is confidence and certainty. No matter the type of communication is physical or electronic. In physical environment, building confidence and certainty is much easy since identifying the entity or person by either direct interaction or certain distinguishing proof may act as marks, public accountant stamp or even the letterhead. In any case, if there should be an occurrence of electronic correspondence, fabricating this trust is very troublesome as the character of the other element stays hid, furthermore the vast majority of the recognizable proof or security strategies that you underestimate in a non-electronic or physical correspondence are not present. This trust can't be set up until and unless both substances are certain about every others personalities and that the data they are trading over a system is totally secure from any sort of altering (Radha *et al*., 2007).

For instance, when you go to a store you are very certain about the authenticity of the organization. You can see and touch the item, you may even know the charging representative and when delivering electronic card to the charging representative you won't not feel the danger of your mastercard being abused in any capacity. However, while trying the same purchasing experience over the internet, you are not exactly beyond any doubt about the authenticity of the organization or the item. You are not by any means beyond any doubt about the personality of the individual to whom you are sending your charge card number.

It is to address these essential issues of assurance, affirmation and security over the framework that PKI is used. PKI brings the security and sureness of the physical world to the electronic world by enabling trusted electronic trades and trades. As talked about in the past part, the center security capacities gave by cryptography are privacy, non-renouncement, verification and respectability. Notwithstanding these center security capacities, it is important to have the accompanying for secure and dependable electronic communications (Sun *et al*., 2007):

- Arrangements that determine rules for working cryptographic frameworks
- Components for overseeing, saving and making keys
- Rules for overseeing, saving, appropriating and making keys and authentications

MATERIALS AND METHODS

PKI components: As discussed in the earlier, PKI is a framework that consists of hardware, software, policies and procedures for handling keys and certificates. For this framework to be functional, you need various components of PKI. These components are shown in Fig. 1.

Certificate Authority (CA): The CA is a trusted outsider unit that verifies substances participating in an electronic exchange. To verify an element, the CA issues a computerized endorsement. This authentication is an advanced report that builds up the qualifications of the elements taking part in an exchange. The advanced declarations issued by CAs contain data for example, the

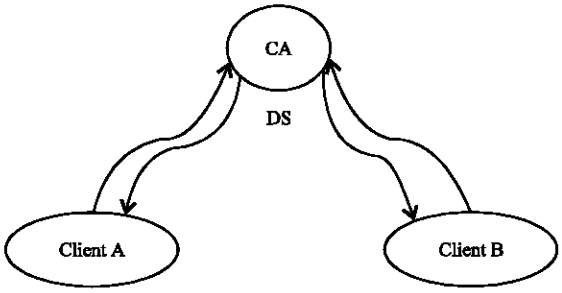

Fig. 1: Components of PKI

name of the supporter, the general population and the private key of the endorser and the issuing CAs open key. This data relies on the arrangement of the organization that issues the endorsements and DSs.

PKI clients: The entities and units requesting CAs to issue certificates are commonly referred to as PKI Clients. To obtain a digital certificate from a CA in the case of WSN those clients are nodes and sensors of WSN.

Digital certificates (DS): As shown in the square by the middle of Fig. 1. It is imperative to guarantee the security of a public key to keep away from security vulnerabilities identified with identity forgery and key alteration. In this way, an information integrity system is required to guarantee that an public key that is altered does not go unnoticed. However, information integrity components alone are not adequate to ensure that public key has is placed with the asserted proprietor. A methodology is needed which ties the general population key with some universally trusted gathering that can guarantee the character and validness of people in general key. The fancied system ought to finish the accompanying two objectives:

- Set up the trustworthiness of the general population key
- Tie public key and its related data to the proprietor in a trusted way (He *et al*., 2007)

Certificate distribution system: The Certificate Distribution System (CDS) disseminates those authentication testimonies to clients and associations. These authentications can be circulated in two routes relying upon execution of PKI in the association. Either the endorsements can be disseminated by clients themselves or they can be appropriated by an index server that utilizations LDAP to question the client data that is put away in a X.500 consistent database. CDs circulate

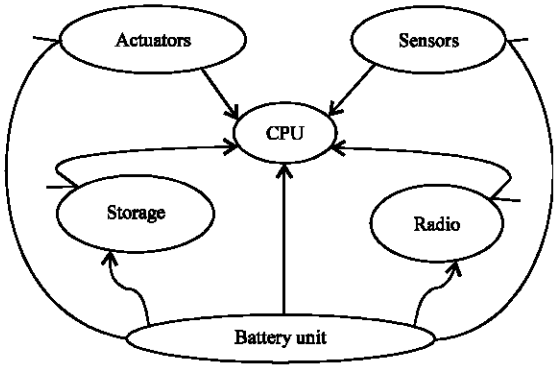

Fig. 2: Sensor architecture

declarations in participation with the index benefit server. The conveyance framework is utilized to do the accompanying tasks:

- Create and claim key pairs
- Affirm the legitimacy of public keys by marking the key
- Revoke expired or lost keys

Chan and Perrig proposed peer intermediaries for key establishment in sensor network called "PIKE". The key is established between the two sensor nodes based on a common trusted third node. For example two nodes of A and B, a node C that share and distribute a key with nodes A and B.

Another deterministic key pre-distribution schemes proposed by Lee and Stinson to enhance the resilience against node/sensor attacks. The major difference between these schemes and other probabilistic methods is that they are based on strongly regular and random graphs correspondingly (Saied and Olivereau, 2016).

WSN: WSN is a collection of sensor nodes to monitor and track certain activity. A sensor might be seen as a very small computing unit or mainly a small unit that is capable of processing storage and transmission as illustrated in Fig. 2, where the blue lines represent power lines where the red lines represent data lines the flow in each case determined through the direction of the arrow.

Applications of WSN: WSNs provides a wide range of applications that range is concentrated on the purpose of monitoring and reporting for example: air traffic control, smart parking, appliance control (lighting and HVAC), traffic flow and congestion control, area and theater monitoring (military), assembly line and workflow,

asset management (e.g., container tracking), battlefield management and surveillance, biological monitoring for agents, blinds assistance, body-worn medical sensors, borders (between countries or cities) monitoring, bridge and highway monitoring (safety) (Maitra *et al*., 2016).

Security in WSN: Security objectives in communication systems rely on upon the need to realize what will be ensured and protected. As a communication system type three principle issues must be carefully mentioned for taking care of security of WSN those issues are requirements, security objectives in a communication systems rely on upon the need to realize what will be ensured and protected. As a communication system type three principle issues must be locations for taking care of security of WSN requirements, dangers and assaults (dangers) and attacks (assaults) (Xie *et al*., 2016).

Security requirements (Saied and Olivereau, 2016): The security requirements of a wireless sensor network are the basic requests those should be found in any communication system they could be classified as follows.

Data freshness: Data freshness recommends that the information is new and it guarantees that no old messages have been retransmitted. This prerequisite is particularly essential when the WSN units utilize shared keys for message transmission where a potential attacker can dispatch a replay attack utilizing the old key as the new key is being transmitted and used to every one of the units in the WSN. The out-dated data contained in the message can bring about numerous issues to the applications in the network system. An illustration is the wormhole attack in WSNs. In this research key freshness is one of the criteria being carefully considered.

Data confidentiality (data classification): Most of application requires some privacy to be guaranteed like surveillance applications, modern business critical information and key/passwords distribution. The standard approach for keeping secrecy is by using encryption. The real issue is that radio range is an open asset and can be utilized by anybody outfitted with appropriate radio handsets. A malignant node can listen to the packets during their transmission as long as that unit can monitor the radio frequencies utilized for the WSN. Another malignant unit creates so called Botnets in which it can reveal the secrets of a unit not by directly attacking it but rather through the information gathered and analyzed from other nodes under its control (zombie units).

Authentication: Trust between nodes and systems. The receiver needs to guarantee that the information is coming from the dependable source. Essentially, validation is vital while transmitting control data over the network. Information validness is an affirmation of the personalities of conveying units.

Time synchronization: With a specific end goal to preserve power, an individual sensor unit might be put to sleep intermittently. Any security methodology for WSN must likewise be time-synchronized.

Availability: Sensor units may come up short on battery control because of overabundance calculation or connections and get to be distinctly inaccessible. It might happen that a malignant unit may overwhelm the sensor to make it inaccessible. The prerequisite of security influences the operation of the network system as well as exceptionally essential in keeping up the accessibility of the system.

Integrity: Content validation is a basic issue while transmitting information over a network system. Information in travel can be changed by the network foes. waste of information can even happen without the act of a malignant unit accidently because of the ruthless connection environment. Information integrity guarantees that the data is not altered in travel, either because of malignant plan or unintentionally. Utilization of message integrity code is usually used as an approach for guaranteeing information integrity.

Self-organization: In WSN, each sensor unit is free and sufficiently adaptable to act naturally arranging and self-recovery as indicated by various struggle situations. Because of the irregular organization of units no settled foundation or infrastructure is accessible for WSN administration. Conveyed sensor network systems must act as self-organized for supporting multi-hop routing. They should likewise act self-organized to lead key administration and building trustable connections among sensors. Various key pre-distribution methods have been proposed regarding to symmetric encryption.

Secure localization: The sensor unit frequently needs area/location data precisely and consequently. However, a malignant node can easily control non secured area/location data by reporting false signal powers and replaying signals and so on.

Security threats and attacks on WSN: The essential classes of attacks against security in sensor systems are

listening/evasdropping, disturbance and hijacking. The listening stealthily is utilized to know the output of sensor units in the system by stealing transmitted messages of sensor unit (Feng *et al*., 2015a, b). There are mostly two approaches to think about output information:

- Passive eavesdropper; this done by hiding from sensor units or
- Active eavesdropper; this done by transmitting queries to sensor unit, root unit or aggregation units

Eavesdropper's location plays an important role in getting data. This attacks influences the property of confidentiality, verification in WSN. So, an appropriate encryption method, message validation codes are required before sending information. The disturbance for the most part impacts results of the system. As per ability of the malignant unit, dangers in WSNs can be arranged into the following classifications.

External vs. internal: An outsider or external attack originates from units which don't belong to the WSN. An outer hacker can't access most cryptographic materials in WSN sensors. Outer attacks may create unauthorized traffic monitoring on information transmissions and additionally can expand its harm to infuse and inject harmful information like virus or a Trojan into the system to overwhelm the system creating more resource consumption arising (DoS) attacks. Despite what might be expected, the inward attack happens when a privileged unit in a WSN carries on in unintended or unapproved ways. Interior attacker or insider is an approved member in the sensor system that looks to disturb operations or make use of WSN resources.

Active vs. passive: Active attacks happen when an attacker tries to create an unauthorized altering in information transmission through their transmission in fact there are three main active attacks that could happen to a WSN.

Modification of messages: Some portion of a legitimate message is illegally updated or that messages are reordered or delayed to produce an illegitimate act later.

Denial of Service (DOS): Prevents or denies the normal use or management of resources.

Masquerade: A unit entity pretends to be a different one as for passive attacks those are the types of attacks on a WSN causing no noticeable damage or harm in fact those are really difficult to be explored, since they only do one of the following (Jia *et al*., 2012).

Message content release: Listening and obtaining the messages contents while they are transmitted.

Traffic analysis: If the attacker couldn't read the message content due to an encryption, it still be useful to him just to create statistics about the flow of information those statistics will help the attacker later to break the encryption mechanism.

Sensor-class vs. unit-class attacks: Sensor class or mote-class is the type of attacks that could happen to a sensor unit or any set of small resources with similar capabilities. Where as in unit class attack the attacker could use more advanced units like laptops or mobile units and can do a great deal more mischief to a system than an illegitimate sensor units. These network elements can transmit with a wider range, process faster and have more strong batteries than the system units. In a WSN, sensors watch and track the progressions of particular parameters or values and answer to the sink as required. While sending reporting, the data in travel might be attacked to give wrong data to the base stations or sinks. The shortcoming in a framework security plan, execution, arrangement or constraints that could be abused by attacker is known as flow or vulnerability (Zhu *et al*., 2012).

Fuzzy rule based systems: Fuzzy Rule-Based Systems (FRBSs) are of the most well-known methodologies within soft computing. FBRS originally based on the fuzzy basis to address complex computing. They have become an outstanding way to tackle various problems such as uncertainty, imprecision and non-linearity. The clearest areas of their implementation are identification, classification and regression tasks (Collotta, 2015).

FRBSs might also be known as fuzzy systems or fuzzy inference systems. The main concepts of FRBSs are based the work of Zadeh on the fuzzy set theory, the goal of this work is to represent knowledge and language of human experts as sets of no deterministic IF-THEN rules. Rather than the use of crisp sets as in classical IF-THEN rules, fuzzy rules use fuzzy sets. The set of fuzzy rules were initially derived from ordinary human experts through knowledge engineering processes. FBRS could be viewed as a system of five steps:

- Step 1: fuzzification in which crisp values are transformed into linguistic values using a transformation function as the shape of the membership function
- Step 2: inference which uses fuzzy set theory to map inputs to outputs
- Step 3: rule strength ratio calculation

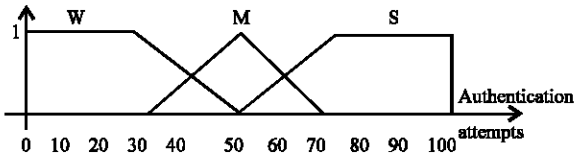

Fig. 3: NH fuzzy rule

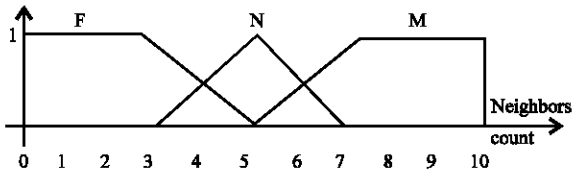

Fig. 4: NTN fuzzy rule

- Step 4: consequent parts parameters calculation
- Step 5: output generation as the cumulative sum of all incoming signals

The proposed paradigm: In this study, a Security algorithm applied to MANETs is presented. This algorithm may be viewed as a two stages: first a fuzzy model to decide the key length for the current session. Then the key distribution between nodes in MANET both stages are illustrated in the rest of this study.

Fuzzy rule based system (key size determination): To offer a secured platform in rapidly changing conditions like WSN it requires great attention. The core of the proposed algorithm is to design a fuzzy function that takes a number of variables then decide the actual number of bits needed after the defuzzification process. To do so the fuzzy logic functions handles three parameters simultaneously: number of nodes currently associated with WSN (NN), takes two values (little and much). The Node history (NH) associated with each node which is in fact a fuzzy variable with one of three values. Week (represents that the entity had been authenticated many times before and causes no vulnerabilities). Medium (represents that the entity had been authenticated medium number times before and causes no or at most 2 vulnerabilities). Strong (represents that the entity had been authenticated one or no times before).

The calculation for the NH is based fuzzy rules using number of authentication attempts done by that entity illustrated in Fig. 3. The bigger number denotes possible vulnerability. Number of Trusted Neighbors (NTN). It has three fuzzy sets few, normal and many. The membership function as shown in Fig. 4.

The neighbor hosts the mobile host has the more potential attacker, i.e., the possibility of attack is greater. There are many other factors affecting the safety of mobile hosts such as bandwidth. The security level of mobile hosts is a function with multiple variables and affected more than one condition.

Key Changing Frequency (KCF), a fuzzy variable with two values {(slow: for normal traffic and minimal number of session key change) and (fast: for heavy traffic and maximum number of session key change)}. The faster change of the session key, more secure the mobile host. It is more difficult to decipher the session key to a shorter time. A mobile host to change the secret key is often safer than a mobile host using a constant secret key.

Session Key Length (SKL): A fuzzy variable with three values short, medium and long In this research the key lengths from 16-512 bits are assumed which is explained as follows:

- Long: the session key is harder to withstand a severe attack of brute force and corresponds to a crisp value 512 bits
- Medium: the session key will correspond to a medium traffic and medium security requirements it will correspond to a crisp value of 256 bits

Short: In this case, the session key will correspond to a minimal traffic with the smallest security requirements and will correspond to a crisp value of 64 bits.

The Security-Level of WSN entity is in direct proportion to the frequency of changing the key and the number of trusted neighbors in its cluster and in inverse proportion to the overall number of neighbor hosts. The SL value is updated by the fuzzy logic system. When the key length is short, the SL of WSN unit should be low; otherwise SL should be high.

The output fuzzy variable "the Security-Level of MS" has five fuzzy sets lowest, low, normal, high and highest. It should be noted that modifying the membership functions will change the sensitivity of the fuzzy logic system's output to its inputs. Also increasing the number of fuzzy sets of the variables will provide better sensitivity control but also increases computational complexity of the system.

The output of that system is then passed into a defuzzification function shown in Table 2 that will decide the number of bits used the accurate key length required for the current state.

Session key distribution: After the key size had been determined by the fuzzy system. It now came to the distribution of the key which poses a great threat to the whole security system, since the key must be

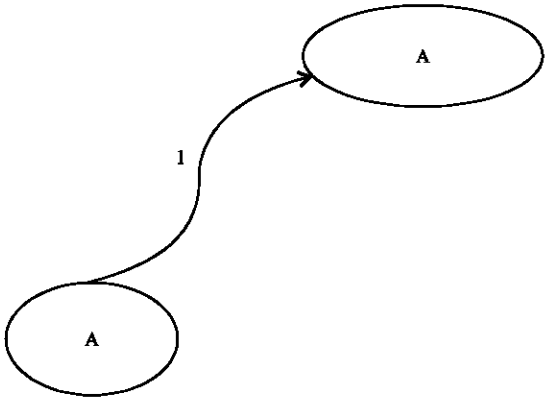

Fig. 5: PK node request

changed according to the network conditions. To achieve that goal a set of currently will known key distribution methodologies put to the test as will be clarified in experimental results section. Depending on the nature of the WSN the Authentication Authority (AA) methodology is chosen as will be clarified in this study.

The key distribution scenario for WSN requires each node to be given a pair of keys public key (KU) and private key (KR) any node tries to connect to another node must follow the steps shown in the key distribution model illustrated as follows (in each graph a curved line means that the message is encrypted where a straight line means a non-encrypted message).

The node (A) sends a request message to the Authentication Authority (in this case the sensor in WSN) that message is encrypted two times firstly with the node KR (to authenticate its self to the AA) secondly with the AA's public key KU_{AA} (this encryption assures that no one other than AA can read the message). This step is illustrated in Fig. 5. That message contains thee tuples:

- ID_a: a special declarative for the entity (A) which is a combination between physical MAC and IP address
- Timing T_1: a nonce to denote the time for the origination of the message to prevent replay attacks
- Enquiry E: indicates the purpose of the message is to obtain the public key of the entity in concern (B)

The AA sensor decrypts the message using the KR_{AA} then with Ku_a (it now assures that the message is generated from A. This step is illustrated in Fig. 6 after analyzing the message the AA sends a message encrypted also 2 times using KR_{AA} for authentication and KU_a the message contains two tuples:

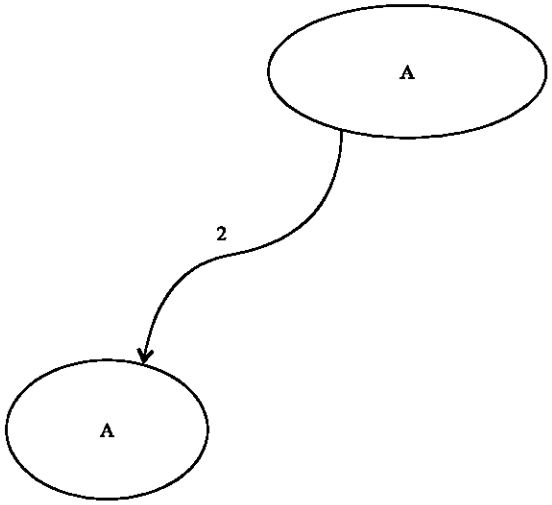

Fig. 6: AA reply to a node

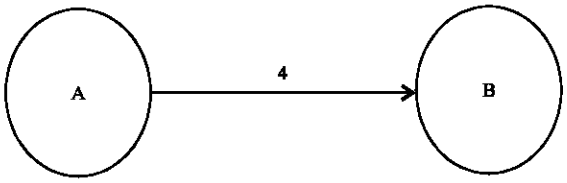

Fig. 7: Node A sends req. to node B

- Timing T_2: a nonce to denote the time for the origination of the message from AA
- KU_b: the public key of desired entity B

A receives the message and decrypts it using KU_{AA} then KR_a after analyzing the message it compares the timing T_1 and T_2 to decide wheatear to accept the message or not. Then, if it decides to accept the message it will accept the corresponding KU_b. A sends a non-encrypted message to the desired node (B) (Fig. 7) contains only two tuples:

- Timing T_3: a nonce to denote the time for the origination of the message from A
- KU_a: the public key of desired entity A

B receives the message and extracts KU_a then sends a request message to the AA this step is illustrated in Fig. 8 that message is encrypted 2 times firstly with the node KR_b (to authenticate its self to the AA) secondly with the AA's public key KU_{AA} (this encryption assures that no one other than AA can read the message). That message contains thee tuples:

- ID_b: a special declarative for the entity (B) which is a combination between physical MAC and IP address

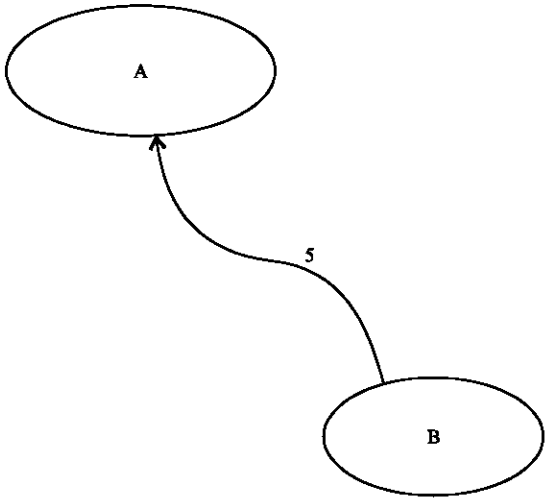

Fig. 8: Node B sends the req. to AA

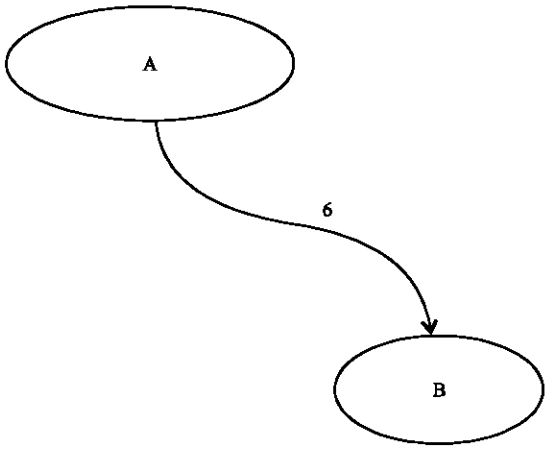

Fig. 9: AA replies to node B

- Timing T_4; a nonce to denote the time for the origination of the message to prevent replay attacks
- Enquiry E; indicates the purpose of the message is to obtain the public key of the entity in concern (A)

The AA sensor decrypts the message using the KR_{AA} then with KU_b (it now assures that the message is generated from B. After analyzing the message the AA sends a message encrypted also 2 times using KR_{AA} for authentication and KU_b. This step is illustrated in Fig. 9 the message contains two tuples:

- Timing T_5: a nonce to denote the time for the origination of the message from AA
- KU_a: the public key of desired entity A

B receives the message and decrypts it using KU_{AA} then KR_b after analyzing the message it compares the

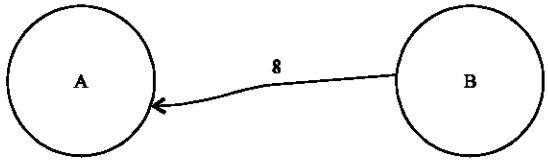

Fig. 10: Node B replies to node A

timing T_4 and T_5 to decide wheatear to accept the message or not. Then, if it decides to accept the message it will accept the corresponding KU_a, now B will compares the public key received from the AA and the one received from A. If the public keys two are same B now is assured that A is authenticated from the AA.

B sends a message to A encrypted 2 times with KU_a then KR_b the message includes only one tuple; timing T_6: a nonce to denote the time for the origination of the message from AA as in Fig. 10.

A receives the message and decrypts it using KU_B then Kr_a after analyzing the message it compares the timing T_3 and T_6 to decide wheatear to accept the message or not. Then, if decides to accept the message it will now be assured that the whole conversation is with B.

Using the fuzzy rule based system A generates the session key and then sends it in a message encrypted 2 times with KU_b then KR_a

RESULTS AND DISCUSSION

While creating this model for securing the transfer of session key, many alternatives had been arises. In this study, the set of experimental results will be clarified. The security model is defined for the experiments is based on three parameters message encryption level, the way to determine the session key and the way to distribute the session key. The alternatives in these parameters are carefully compered based on two main criteria.

The average security level achieved: This parameter is measured through the number of falsely rejected nodes (false negatives) and the number of falsely accepted attackers (false positives).

Processing time: A very important criteria in WSN since it doesn't affect the processing delay of the system only, it also affects the battery of each node in the network since the processing time after certain threshold directly proportional to the battery consumption exponentially. So, this factor had to be managed carefully.

Message encryption level: In this type of experiments two alternatives arrives the first is to create the encryption

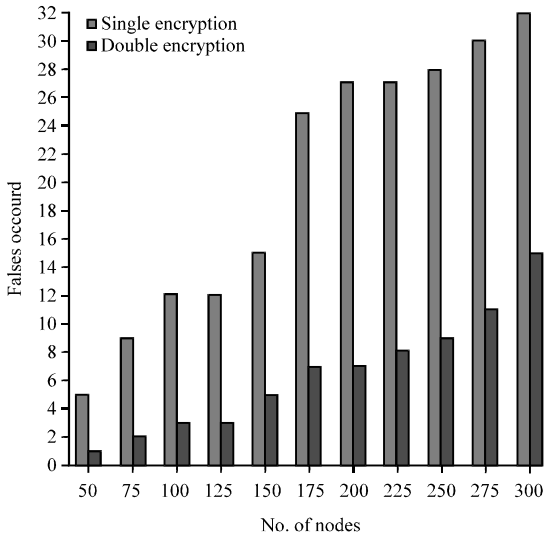

Fig. 11: Message encryption level false positives

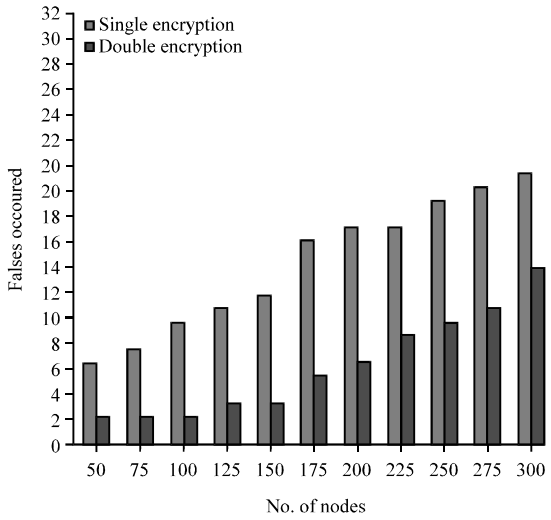

Fig. 12: Message encryption level false negatives

Table 1: The rules used in the fuzzy logic system

SL	NH	KCF	NTN	SKL	NN
Low	Week	Slow	Few	Medium	Little
Lowest	Week	Slow	Medium	Long	Much
Lowest	Medium	Slow	Many	Short	Little
Normal	Strong	Fast	Few	Long	Much
Low	Medium	Fast	Medium	Short	Much
Low	Medium	Fast	Many	Medium	Little
High	Week	Slow	Few	Long	Much
Normal	Medium	Fast	Medium	Medium	Much
Low	Week	Slow	Many	Short	Little
Highest	Medium	Fast	Few	Long	Much
High	Strong	Fast	Medium	Medium	Much
Highest	Strong	Fast	Many	Medium	Much

Table 2: Defuzzification for the values of S

SL fuzzy value	Lowest	Low	Normal	High	Highest
Key bits	8	24	32	64	128

only 1 time using the destination public key only (the public key only) this way provides only encryption to the message in a way such that only the destination can read the message. The second alternative is to make another encryption using the source private key (this provides authentication such that the destination uses the source's public key to decrypt the message by doing so it assures that the message arrives from the exact source) followed by another encryption using the destination public key (this provides only encryption to the message in a way such that only the destination can read the message).

Average security levels: The number of false positives and negatives provided in each case represented in Table 1, 2 and Fig. 10, 11. As Table 3, 4 and Fig. 11, 12 illustrates the advantages of using double encryption over single encryption this is one reason for choosing double encryption.

Table 3: Message encryption level false positives

	False positives	
Number of nodes	Single encryption	Double encryption
50	5	5
75	9	9
100	12	12
125	12	12
150	15	15
175	25	25
200	27	27
225	27	27
250	28	28
275	30	30
300	32	32

Table 4: Message encryption level false negatives

	False negatives	
Number of nodes	Single encryption	Double encryption
50	2	6
75	2	7
100	2	9
125	3	10
150	3	11
175	5	15
200	6	16
225	8	16
250	9	18
275	10	19
300	13	20

Processing time: The idea of applying single or double encryption is based on the need to provide either encryption only or encryption and authentication, the results of applying both cases to the steps of entity authentication to the AA are shown in Table 5 and demonstrated in Fig. 13 and measured in milliseconds.

Table 5 and Fig. 14 shows that the required in the case of single encryption is less than the case of double

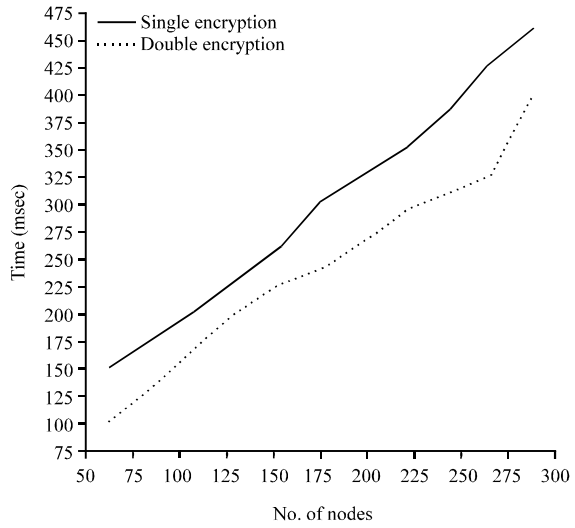

Fig. 13: Message encryption level processing time

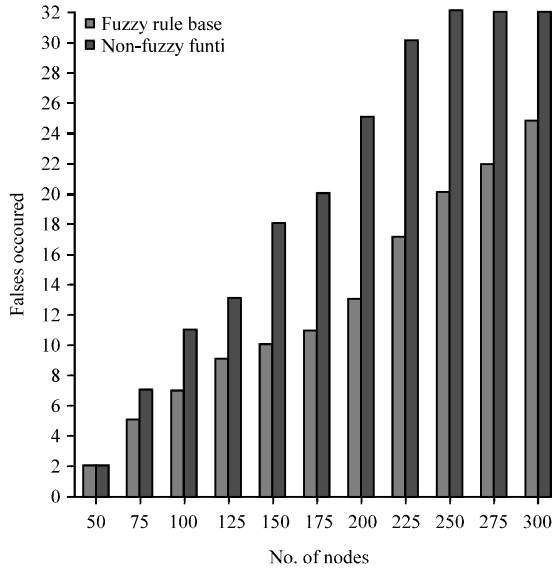

Fig. 14: Session key length determination false positives

Table 5: Message encryption level processing time

Number of nodes	Single encryption	Double encryption
50	100	150
75	130	175
100	165	200
125	200	230
150	225	260
175	240	300
200	265	325
225	295	350
250	310	385
275	325	430
300	400	460

encryption which makes sense because the amount of calculations required in the first case are about half

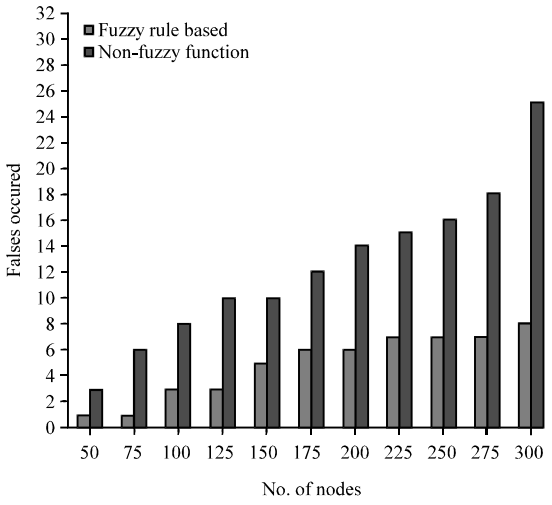

Fig. 15: Session key length determination false negatives

Table 6: Session key length determination (false positives)

	False negatives	
Number of nodes	Fuzzy rule based system	Non-fuzzy function
50	2	2
75	5	7
100	7	11
125	9	13
150	10	18
175	11	20
200	13	25
225	17	30
250	20	33
275	22	37
300	25	40

of the second case. But this difference in time could be neglected opposing to the security level guaranteed by the double encryption. For this reason the double encryption will still be preferred.

Session key length determination: Another important factor arises while creating the system. The length of the key, a non-fuzzy function that directly allocates the length of the key according to the WSN conditions is used and a fuzzy function also implemented to do the job. The results of implementing both cases are illustrated in the current study.

The average security levels: After implementing the fuzzy and the non-fuzzy functions, the results are recorded and the security levels in each case are shown by monitoring The number of false positives and negatives provided in each case these results are represented in Table 6, 7 and Fig. 15, 16.

Table 6, 7 and Fig. 15, 16 illustrate the reason behind the choice of a fuzzy rule based system over the non-fuzzy function the main reason behind those results

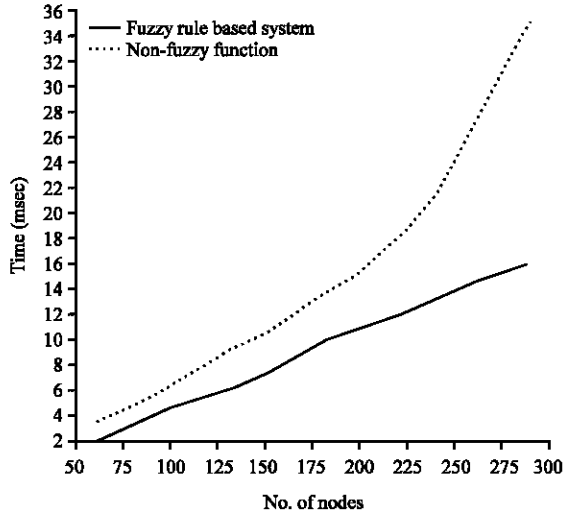

Fig. 16: Session key length determination creation time

Table 7: Session key length determination (false negatives)

	False negatives	
Number of nodes	Fuzzy rule based system	Non-fuzzy function
50	3	3
75	6	6
100	8	8
125	10	10
150	10	10
175	12	12
200	14	14
225	15	15
250	16	16
275	18	18
300	25	25

Table 8: Session key length determination (creation time)

Number of nodes	Fuzzy rule based system	Non-fuzzy function
50	2	3.5
75	3.5	5
100	5	7
125	6	9
150	7.5	10.5
175	9.5	13
200	11	15
225	12	18
250	13.5	22
275	15	28
300	16	35

is flexibility provided by the fuzzy logic in general that flexibility allows the system to keep in mind more variables together at once corresponding to the nature of the WSN.

Creation time: The time required to produce the final Session Key (SKCR) is a very important factor as mentioned earlier and hence it is measured in both cases for single and double encryption and measured in milliseconds the results are shown in Table 8 is illustrated in Fig. 17.

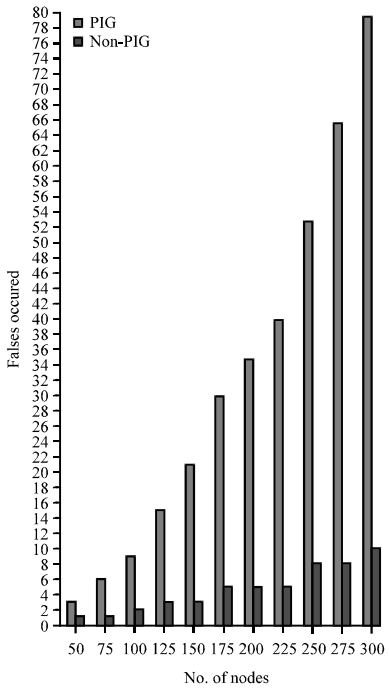

Fig. 17: Key distribution scenarios false positives

The fuzzy rule based system consumes a little bit of time more than the non-fuzzy function as shown in Table 8 and Fig. 17. But the fuzzy system still preferable since that it keeps track and handles various amount of parameters simultaneously also provides a dynamic range of values other than the non-fuzzy function. Table and figure illustrates the results of applying both techniques. The reason of choosing a fuzzy rule based system in despite of the time advantage of the non-fuzzy function is that the huge amount of difference in the security levels provided by the fuzzy system.

Key distribution scenarios: The purpose of the public key encryption is to make it computationally infeasible or almost impossible to generate one key using the other. To choose among the different existing key distribution scenarios the PKI is applied along with the ordinary non-PKI. The results of applying both methods are demonstrated in this study.

Average overall security: The security provided through key distribution might be seen as the difference in false negatives and positives given by each distribution scenario. The results of comparing the outcomes of applying a PKI distribution and a non PKI are illustrated in Table 9, 10 and clarified by Fig. 15-17.

The huge amount of difference in the security level provided by both methodologies as demonstrated in

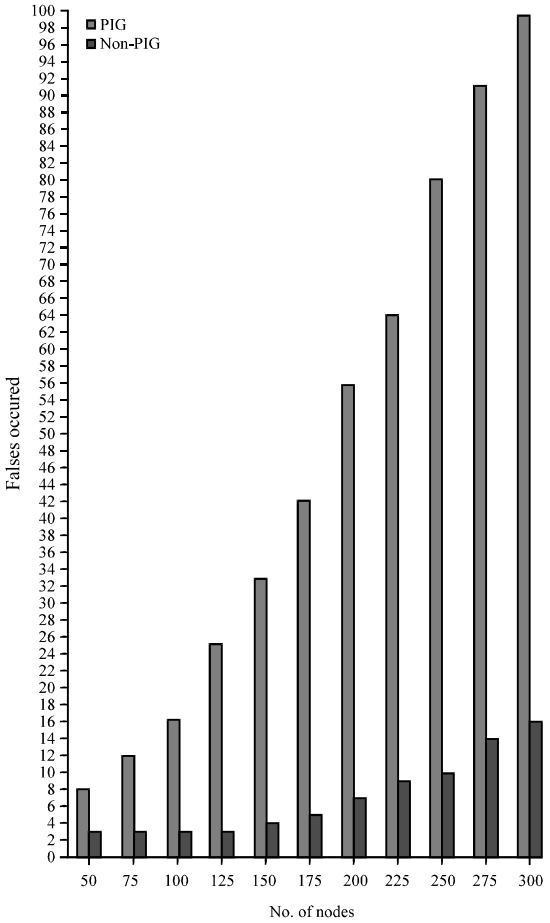

Fig. 18: Key distribution scenarios false negatives

Table 9: Key distribution scenarios (false positives)

	False positives	
Number of nodes	Non-PKI	PKI
50	3	1
75	6	1
100	9	2
125	15	3
150	21	3
175	30	5
200	35	5
225	40	5
250	53	8
275	66	8
300	80	10

Table 9, 10 and visually shown in Fig. 18 and 19 suggest that the use of PKI will be more secured than the non-PKI. The reason here is that PKI makes the attempts to break the cipher very difficult.

Processing time: The PKI in general consumes more time than ordinary methods but in the case of this specific systems the results are close as illustrated in Table 11 and clarified by figure and measured in milliseconds.

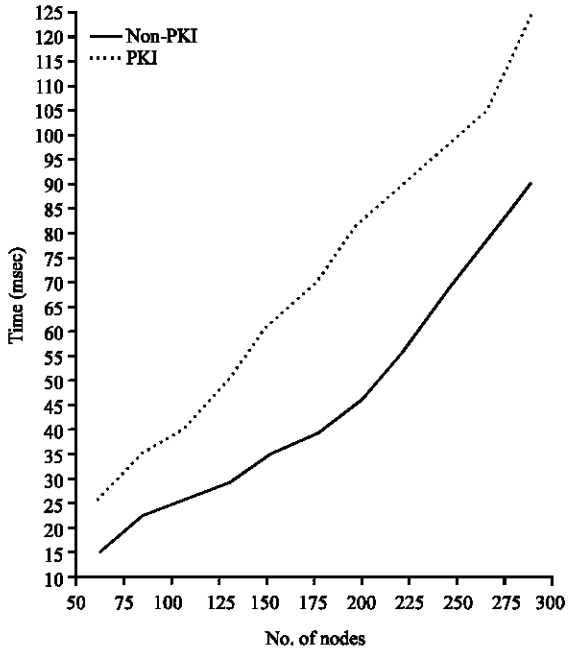

Fig. 19: Key distribution scenarios processing time

Table 10: Key distribution scenarios (false negatives)

	False negatives	
Number of nodes	Non-PKI	PKI
50	3	8
75	3	12
100	3	16
125	3	25
150	4	33
175	5	42
200	7	56
225	9	64
250	10	80
275	14	91
300	16	99

Table 11: Key distribution scenarios (processing time)

Number of nodes	Non-PKI	PKI
50	15	26
75	22	35
100	26	40
125	29	50
150	35	62
175	39	70
200	45	82
225	55	89
250	68	96
275	79	105
300	90	124

Although, Table 11 and Fig. 20 dedicate that the time required deliver the session key using non-PKI is relatively small comparing to the PKI but this time is to neglected while mentioning the higher security level provided by the PKI.

CONCLUSION

WSN is a very important type of networks. It provides applications and connectivity in positions and locations that could be dangerous or out of human reach. Numerous applications could use the nature and advantages of WSN such as traffic surveillance, digging using robotics, etc. These applications and others requires a high level of security to maintain the efficiency and reliability of WSN. In this research a new paradigm of securing session key transmission is proposed. The proposed mechanism provides security to the transmission of session key through fuzzy rule based system which determines the accurate key length depending on the current WSN conditions. After the key length has been accurately determined PKI by double encryption had been used. The complexity of the mechanism provides more security level with a slight amount of increasing time which is ignored comparing to the security level provided.

SUGGESTION

As a future work it is possible to apply concepts of intuitionistic sets and other types of fuzzy logic. It is also possible to apply the mechanism to other wireless networks.

REFERENCES

Collotta, M., 2015. FLBA: A fuzzy algorithm for load balancing in IEEE 802.11 networks. J. Netw. Comput. Appl., 53: 183-192.

Elmazi, D., S. Sakamoto, T. Oda, E. Kulla and E. Spaho *et al*., 2016. Effect of security parameter for selection of actor nodes in WSAN: A comparison study of two fuzzy-based systems. Proceedings of the 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA'16), March 23-25, 2016, IEEE, Crans-Montana, Switzerland, ISBN:978-1-5090- 1857-4, pp: 957-964.

Feng, T.H., W.T. Li and M.S. Hwang, 2015a. A false data report-ltering scheme in wireless sensor networks: A survey. Intl. J. Netw. Secur., 17: 229-236.

Feng, T.H., N.Y. Shih and M.S. Hwang, 2015b. A safety review on fuzzy-based relay selection in wireless sensor networks. Intl. J. Netw. Secur., 17: 712-721.

Hanafy, I.M., A.A. Salama, M. Abdelfattah and Y. Wazery, 2012. Security in MANET based on PKI using fuzzy function. IOSR J. Comput. Eng., 6: 53-58.

Hanafy, I.M., A.A. Salama, M. Abdelfattah and Y.M. Wazery, 2013. AIS model for botnet detection in manet using fuzzy function. Int. J. Comput. Networking Wireless Mobile Commun., 3: 95-102.

He, W., X. Liu, H. Nguyen, K. Nahrstedt and T. Abdelzaher, 2007. PDA: Privacy-preserving data aggregation in wireless sensor networks. Proceedings of the 26th IEEE International Conference on Computer Communications, May 6-12, Anchorage, pp: 2045-2053.

Inaba, T., D. Elmazi, Y. Liu, S. Sakamoto and L. Barolli *et al*., 2015. Integrating wireless cellular and ad-hoc networks using fuzzy logic considering node mobility and security. Proceedings of the 2015 IEEE 29th International Workshops on Advanced Information Networking and Applications (WAINA'15), March 24-27, 2015, IEEE, Gwangiu, South Korea, ISBN:978-1-4799- 1775-4, pp: 54-60.

Jia, Z., X. Lin, S.H. Tan, L. Li and Y. Yang, 2012. Public key distribution scheme for delay tolerant networks based on two-channel cryptography. J. Netw. Comput. Appl., 35: 905-913.

Karlof, C. and D. Wagner, 2003. Secure routing in wireless sensor networks: Attacks and countermeasures. Ad Hoc Networks, 1: 293-315.

Kulla, E., G. Mino, S. Sakamoto, M. Ikeda and S. Caballe *et al*., 2014. FBMIS: A fuzzy-based multi-interface system for cellular and ad hoc networks. Proceedings of the 2014 IEEE 28th International Conference on Advanced Information Networking and Applications (AINA'14), May 13-16, 2014, IEEE, Victoria, British Columbia, Canada, ISBN:978-1-4799-3630-4, pp: 180-185.

Maitra, T., R. Amin, D. Giri and P.D. Srivastava, 2016. An efficient and robust user authentication scheme for hierarchical wireless sensor networks without tamper-proof smart card. Intl. J. Netw. Secur., 18: 553-564.

Radha, P., W. Cliff and R. Sumit, 2007. Secure Localization and Time Synchronization for Wireless Sensor an Ad Hoc Networks. Springer, New York.

Saied, Y.B. and A. Olivereau, 2016. A lightweight threat detection system for industrial wireless sensor networks. Intl. J. Netw. Secur., 18: 842-854.

Sun, B., L. Osborne, Y. Xiao and S. Guizani, 2007. Intrusion detection techniques in mobile ad hoc and wireless sensor networks. IEEE Wireless Commun., 14: 56-63.

Xie, Q.Q., S. Jiang, L. Wang and C.C. Chang, 2016. Composable secure roaming authentication protocol for cloud-assisted body sensor networks. Intl. J. Netw. Secur., 18: 816-831.

Zhu, W.T., J. Zhou, R.H. Deng and F. Bao, 2012. Detecting node replication attacks in wireless sensor networks: A survey. J. Network Comput. Appl., 35: 1022-1034.