Secure Hierarchal Routing Protocols in Wireless Sensor Networks; Security Survey Analysis

Ali Modirkhazeni, Norafida Ithnin, Mohammadjavad Abbasi

Abstract—Wireless Sensor Network is consisting of number of limited sensor devices which are communicated over the wireless media. There are a lot of its application in military, health and industry. As sensor devices are resource restricted, the networks exposed to different types of attacks and conventional techniques against these attacks are not desirable due to the resource constrained nature of these kinds of networks. Therefore, security in WSNs is a challenging task due to inheritance limitations of sensors and it becomes a good topic for researchers. In this paper we focus at secure hierarchal routing protocols in wireless sensor networks and represent selected approaches which focusing at this matter. Finally we develop a matrix which generalizes previous works and analyze the proposed matrix and then suggests the protocols to be applied in proper application.

Index Terms— Secure Hierarchal Routing Protocol, Security, Wireless Sensor Network, Security Matrix.

1 Introduction

WIRELESS Sensor Network (WSN) is a growing technology which is offering solution to variety of application areas such as health care, military and industry. These kinds of networks usually apply number of devices known as sensor devices. These sensors which are limited are distributed over the environment and communicate through the wireless media. They are also responsible of sensing environment and transmission information as well. Usually the transmission task is critical as there are huge amount of data and sensors devices are restricted. As sensor devices are limited the network exposed to variety of attacks. Conventional security mechanisms are not suitable for WSNs as they are usually heavy and nodes are limited.

The rest of the paper is organized as follow: Section 2 presents wireless sensors applications and comes up with the matrix which classifies the WSN's applications. Section 3 will review the sensor node architecture. Routing taxonomy will be presented in the next section and Section 5 briefly review security issues in WSNs. After that we focusing on secure hierarchal routing approaches in wireless sensor networks and survey selected ones. Then Section 7 generalizes selected approaches and proposed selected protocols for appropriate applications. Finally Section 8 concludes the paper.

- *PhD Student, Faculty of Computer Science and Information System, University Technology Malaysia, 81310 UTM Skudai, Johor Darultakzim, Malaysia*
- *Senior Lecturer, Faculty of Computer Science & Information Systems, University of Technology Malaysia. 81310 UTM Skudai, Johor Darultakzim, Malaysia*
- *PhD Student, Faculty of Computer Science and Information System, University Technology Malaysia, 81310 UTM Skudai, Johor Darultakzim, Malaysia*

2 Applications of Wireless Sensor Networks

Nowadays there are many of WSN applications in industry, military and health care. According to functionality of network we can classify WSN's applications into: into Event Detection and Reporting, Data Gathering and Periodic Reporting, Sink-initiated Querying and Tracking-based Applications [1]. In the event detection and reporting applications such as intruder detection systems in military, detecting unusual behavior or failures in a manufacturing process or detection of forest fires, the infrequency of occurrence of specific events has been detected via WSN. In data gathering and periodic Reporting applications such as monitoring temperature, humidity and lighting in office buildings, data gathered and reported in the specific periods of time. In sink-initiated querying scenarios the process of gathering and reporting environment data had been asked through the base, or sink. In tracking-based application such as surveillance, WSN may be used in order to track of specific objects in the environment.

According to the domain of application we can classify WSN application into Environmental, Industrial, Healthcare and Security/Critical applications. This classification is shown in Fig. 1.

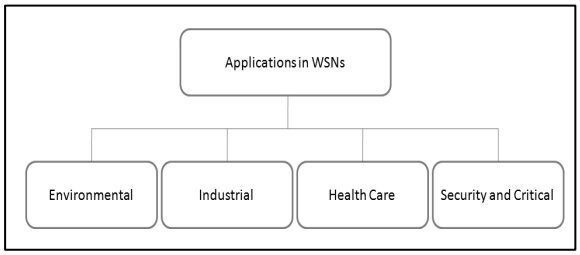

Fig 1. Classification of WSN applications

Environmental application such as structure monitoring, habit monitoring and underground monitoring usually verifications will be done on the specific environment or the things inside that environment. In the industrial application such as control process application, wireless sensor network technology will be applied in the industry. Healthcare is another classification which applies WSN solutions to variety of applications such patient monitoring. WSNs are also being applied in security application such as boarder surveillance or intruder detection system.

3 Sensor Device Architecture

Perhaps the most widely used element in wireless sensor networks is sensor device, also may be referred as sensor node or node. Sensor nodes in WSNs are responsible of both sensing environment data and transmission as well. They are usually consisting of limited processor, memory, battery, sensor(s) and transceiver. Verdone et al. consider the five elements for sensor device which are shown in Fig 2.

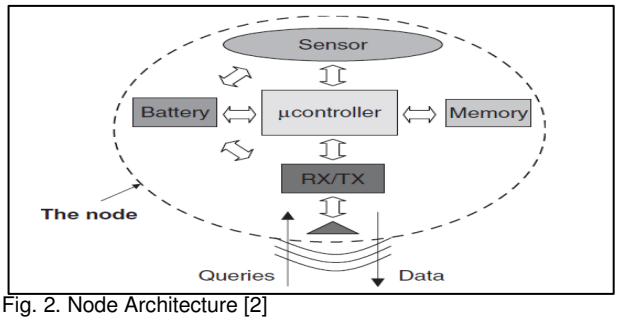

Fig. 2. Node Architecture [2]

According to [2], sensor node device has the Microcontroller which handles tasks. It also has memory which is used to store sensed data. The radio transceiver applied to transmit data. Additionally it has the sensor(s) to sense environment. And finally the power source, the battery, which is used to provide required power for the other elements.

4 Routing In Wireless Sensor Networks

As it mentioned in Section 3, sensor devices are usually restricted in case of memory, processor and power. Additionally they are responsible for sensing and transmission of data as well. Data transmission task is critical and challenging as there are usually huge amount of data and sensor devices are limited. So designing the routing protocol for these kinds of networks should consider these limitations in mind.

Routing protocols as it is illustrated in Fig. 3 can be categorized into the following categories base on how protocol selects the next hop for packet forwarding [3]: Content-base routing protocols which in order to forward the data, selects the next node base on the content of the query, this query usually issues by sink. Another category in this classification is probabilistic routing protocols which randomly select the next hop in order to mitigate the load and improve the robustness of the network. Location-based routing protocol is also placed in this classification. These kinds of protocols select the next hop base on the position of the destination and neighbors as well. Hierarchical-based routing protocols are in this category as well. Sensor nodes in hierarchal routing protocols, forward the data to a node(s) which is placed in the higher hierarchy than the sender, this sensor node is called aggregator, and then be forwarded to base via aggregators. Another category in this classification is Broadcast-based routing protocols which every sensor node individually decides to forward the data or to drop it. If it wants to forward the data, it simply broadcast it again.

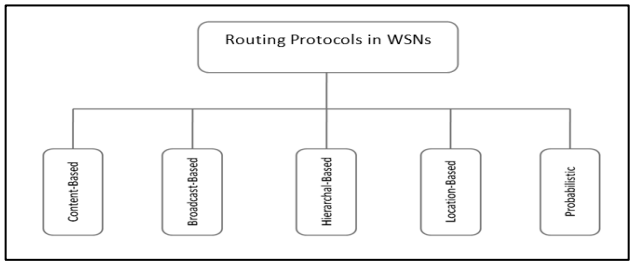

Fig 1. Illustration of Acs and Butty's routing protocols classification in WSNs

In another classification routing protocols in wireless sensor networks were classified into Data-Centric, Flat, QoS-Based, Geographical, Multipath and hierarchal base on the deployment of the network [4]. . In data-centric routing, usually sink ask for specific node data by broadcasting a message. After this message is reached to the specific node which sink is interested in its data, it will send the information back to sink.

Flat routing uses tremendous equal sensor nodes (in case of memory, processor and so on) which collaborate together in order to sense the environment. In the QoS-based routing, routing is performed by applying QoS parameters which usually control packet overhead and energy efficiency.

Geographical routing uses location information of the

node to forward data. By applying this approach, overhead may significantly decreases. In the multipath routing, multiple paths from source to destination are created and packets will send to destination through these paths. In the hierarchal routing (also called as cluster-based routing), the virtual tree is made by the nodes. Each node sends the packet to base (root of the tree) through the parent node. This classification is shown in the Fig. 4.

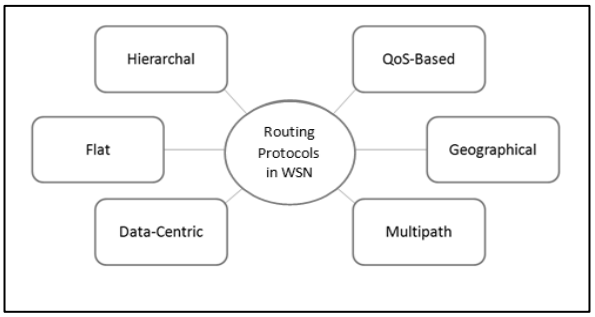

Fig 2. Illustration of Boukerche et al routing classification in wireless Sensor Network

In this section some different points of view concerning with routing classification in wireless sensor networks were represented. They were different from each other as they were made considering different factors such as deployment of network and protocol functionality.

5 Security Issues in Wireless Sensor Networks

Security will be critical in WSNs and achieving security objectives is a challenging task as resources are limited in wireless sensor networks. Many of traditional security techniques are not desirable for WSNs due to the resource constrained nature of these kinds of networks. Brief introduction of security issues is presented in this section.

5.1 Basic Security Requirements in Wireless Sensor Networks

In order to achieve security in wireless sensor networks security requirements should be provided. These security requirements are as follow, system may satisfy some of these requirements depend on application [5], [6], [7] and [8]. The basic security requirements in WSNs are shown in Fig. 5.

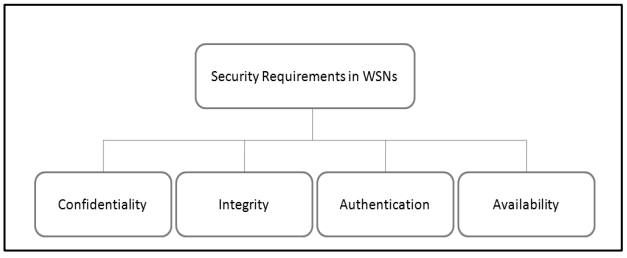

Fig 3. Basic Security Requirements in WSNs

Confidentiality is the ability of hiding message to an unauthorized attacker. It means that if an illegal and unauthorized adversary access to the message, it cannot understand it. Integrity provides a mechanism in order to know whether the message had been tampered or not.
Authentication is ability to identify the reliability of message origin.
And availability grantees that network services are on hand as they needed. This factor identify whether message can move on to network or not. If the node can use its resource, then the availability is provided to the network for forwarding the message.

Although security in wireless sensor networks depends on the application, there are some basic security requirements which proposed by researchers. System may satisfy some of them as it needed. We try to extract minimum security requirements for different types of application in sensor networks which is mentioned in Section 2 and illustrated in Fig. 1. Table 1 illustrates the security requirement regarding to different application categories.

TABLE1
ILLUSTRATION OF SECURITY REQUIREMENTS REGARDING TO DIFFERENT APPLICATIONS IN WSNS

Application	*Basic Security Requirements*			
	Confidentiality	Integrity	Authentication	Availability
Environmental		×	×	
Industrial		×	×	
Healthcare	×	×	×	×
Security/Critical	×	×	×	×

As it is illustrated in Table 1, different kinds of application in WSN, need different level of security. Base on study of [9], [10] , [11] , [12] and [13] authentication and integrity is the minimum basic security requirements which should be satisfied to make environmental applications such as habit monitoring and industrial applications such as controlling process be reliable. Healthcare application should keep patients confidential. The reliability of these systems are also very important so the authentication, integrity, avaiablity and confidentiality is the minimum security requirements that should be achieved in healthcare applications [14], [15], [16], [17], [18], [19], [20], [21] , [22], [23]. Security and critical application such as intruder detection and boarder surveillance should satisfy maximum level of basic security requirements [24], [23],

[25].
Therefore the security in wireless sensor network is depending on the application and different types of application needs different levels of security. Consequently system may satisfy some basic security requirement as it required.

5.2 Routing Attacks in Wireless Sensor Networks

Due to the limitations of resources in wireless sensor networks, these kinds of networks exposed to variety of attacks. Routing attacks which target the network layer in wireless sensor networks are shown in Fig. 6 and the brief description of them will be presented in this subsection [6], [7], [26], [27], [8] and [5].

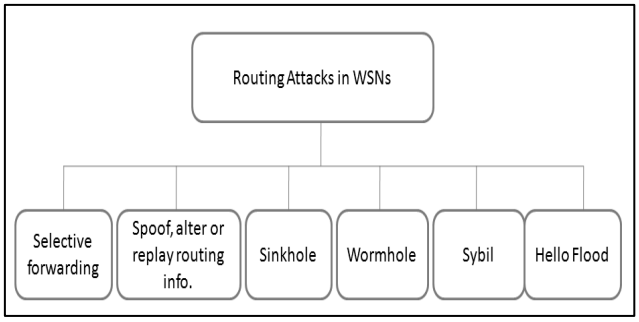

Fig 4. Routing Attacks in WSNs

In selective forwarding attack, certain messages will be dropped by malicious node. Two factors are important in this attack. First is location of attacker, if the location of malicious node is close to base, it will attract more traffic. Another factor is the amount of dropped messages, the more it drops, the more energy it has in order to attack. In the case of sinkhole attack, also known as black-hole attack, attacker surprisingly announces the short path to sink in order to attract traffic. And when it attracts the messages drop them or run selective forwarding attack.
In scenario of Spoofed, Altered or replayed routing information, attacker targets at the routing information as it exchanged among neighbors. In this case, attacker may spoof, alter or replay the routing packets, creates the loops in networks, repel the network traffic and etc. The adversary in Sybil attack announces multiple identities by fabricating and stealing the identity of the legal nodes. The fast tunnel will made by adversary attacker in wormhole attack. The attacker will forward the traffic of one place in the network to another place through this tunnel in wormhole attack. In case of hello flood attack, attacker broadcasts Hello message with the strong transmission power to the networks and make itself as a fake sink.

5.3 Cryptographic approaches in Wireless Sensor Networks

Sometimes malfunctioning of network is not aim of the attacker; instead it has intent of accessing and interpreting the data which it collected. Therefore in order to prevent attacker from eavesdropping, cryptography will be applied. Cryptography, simply, aims at making data not understandable to an unauthorized adversary which has the goal of data interpretation. In order to apply cryptography in any system including wireless sensor networks, cryptographic keys should be distributed among the parties, sensor node in this case, and this task is the responsibility of key management system. Cryptographic algorithms use these keys for data encryption and decryption. Depending on the key, there are two types of cryptography: symmetric cryptography - mostly referred as secret key cryptography - which will use the same key for encryption and decryption and asymmetric cryptography, also known as public key cryptography, which uses public/private pair key for encryption and decryption. Conventional public key cryptographic algorithms are not desirable for wireless sensor networks due to the limited resources [28], [8], [29] and [30].
Unlike public key cryptography, symmetric cryptographic techniques more be used in wireless sensor networks. There are some symmetric encryption algorithms which are also used in wireless sensor networks [31], [32] and [33] [34]. Table II, shows some of these algorithms accompany with their features.

TABLE 2
CRYPTOGRAPHIC ALGORITHMS IN WSNS

Name	Key length	Block Length
AES [35]	128 bits	128 bits
RC5 [36]	128 bits	64 bits
RC6 [37]	128 bits	128 bits
Misty1 [38]	128 bits	64 bits

Law et al. tried to evaluate these algorithms on wireless sensor networks. According to their findings, AES is more desirable in order to providing high security and efficient energy consumption. They also claimed that Misty1 is more suitable for good memory and energy efficiency. This is against some of other works such as [31], which rather to use RC6 as the cryptographic algorithm.
Choosing cryptographic method in wireless sensor networks is critical task due to the resource constrained nature of these kinds of networks. It should be chosen concerning with the factors such as energy consumption efficiency and required memory and security level. Electing unsuitable cryptographic scheme and algorithm for wireless sensor network consequences the negative effect on network.

5.4 Key Management Approaches in Wireless Sensor Networks

In order to perform cryptographic operation on data in any cipher system, it is needed to distribute the corresponding keys among the parties. And this is the goal of key management system. In the sensor networks, key management protocols are the core of secure communication and they are focusing at making the secure connection between two nodes. These will be happened by establishment and distribution of keys among the parties. Depending on cryptographic schemes we can have Symmetric and Asymmetric key management protocols in wireless sensor networks. (Although some protocols use the combination of these two schemes such as [39]). The brief introduction of symmetric key management schemes is presented as follow.

Symmetric key management approaches as they need less computation time are more desirable to apply in wireless sensor networks. Here are some symmetric key management schemes in wireless sensor network: Entity base, Pair-wise, Pure probabilistic, Polynomial based, Matrix based and Tree based key pre-distribution schemes. Fig. 7 illustrates symmetric key management schemes in wireless sensor network.

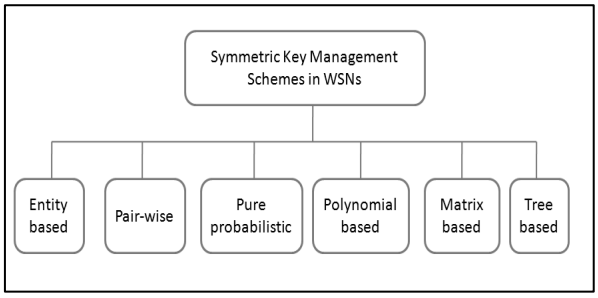

Fig 5. Symmetric Key Management Schemes in WSNs

In the entity based schemes such as [40] and [41] key establishment and distributions will be done by trusted entity. Pair-wise key management schemes such as [42] pair wised key between neighbors is distributed and stored directly in the sensor nodes before network will be deployed. Pure probabilistic key managements protocols such as [43] which mostly be referred as the basic scheme distribute the key among the parties concerning the given probability so nodes do not need huge amount of memory to store the keys. Basic scheme has three phases which are key pre-distribution, shared-key discovery, and path key establishment. This phase ensures that any two nodes share at least a key with a chosen probability; for example in order to have a probability of 0.5 only 75 keys should be drawn out of a key pool with the length of 10,000 to form any key ring. The second phase is responsible of discovery of the neighbors in the sensor network. Finally the last phase is focusing at assigning a path-key to select those sensor nodes in network that do not share a key but are connected by two or more communication links at the end of the shared-key discovery phase.

Polynomial based key management schemes which first proposed by Blundo et al. [44] and based pair wise approach, use the polynomial mathematics in order to generate key pool and key assignment among the parties. In the matrix based key pre-distribution schemes such as [45] the matrix K_{n*n} is responsible of storing all pair wise keys. The element k_{ij} represents the shared key between node i and j in the network. This matrix is made under the condition which says the element k_{ij} is equal to element k_{ji}. $K = (DG)^T G$, where $D_{(l+1)*(l+1)}$ and $G_{(l+1)*n}$. G is known as public matrix and $(DG)^T$ is called secret matrix so must be confidential to all nodes. In order to generate the pair wise key, node i only store i-th row of secret matrix. And after deployment of network nodes i and j compute the shared key $k_{ij} = k_{ji}$ by exchanging their stored rows.

In the tree base schemes, key generation and distribution will be done base on the tree structure. As an example in deterministic key pre distribution which is proposed by Lee and Stinson [46] uses regular graph and one way hash function in order to generate the keys and store (not entire keys) them in the nodes.

Asymmetric schemes are mostly based on RSA and elliptic curves cryptography which are two widely used public key cryptographic techniques consider being heavy to be applied in WSNs. Although symmetric key management protocols are more desirable to be applied in wireless sensor network there are some researches such as [47] and [48] show asymmetric schemes are also viable in these kinds of networks and .

As the summary of this subsection, depending upon the cryptographic scheme we can have symmetric and asymmetric cryptographic protocols in wireless sensor networks. Symmetric key management approaches are more suitable to be applied in WSNs as they have less computational time even though asymmetric key management approaches are also viable in sensor networks.

In this section variety of issues regarding to the security in wireless sensor networks were reviewed. You were familiar with security requirements in WSNs in the first subsection. After that brief introduction of attacks in sensor networks were presented in the second subsection. Next subsection reviewed cryptographic approaches in WSNs and the last one briefly presented key management approaches in these kinds of networks. In order to provide security for routing protocol in wireless sensor network, these issues should be considered.

6 Secure Hierarchal Routing Protocols in Wireless Sensor Networks

Although there are many routing protocols proposed for wireless sensor networks, few of them consider the problem of security and most of them developed without any

security consideration. In this subsection, we go through the secure hierarchal routing protocols which have been proposed for wireless sensor network, and we review ten of them.

Yin and Madria proposed hierarchical secure routing protocol against black hole attack (HSRBH). This protocol is the family of hierarchical routing protocols which applies MAC (Message Authentication Code) for integrity of the packets and Symmetric cryptography for discover a safe route against black hole attack. In this approach first network is divided into set of groups. Each group has its own leader. So there are two types of shared key in HSRBH: *inter-group key* which is shared between two group leaders and *intra-group key* which is shared among neighbors of leader. This protocol uses *Randomized Data Acknowledgment* to defend against black hole attack which attacker drops the packets that forwarded to sink. In this protocol, source asks sink (destination) to send an acknowledgment and sink will send the acknowledgment to source. If source receive this acknowledgment and verification process is successfully accomplished, route is secure against the black hole attack.

Du et al. proposed A Secure Routing Protocol for Heterogeneous Sensor Networks (TTSR) to provide security attributes such as confidentiality, authentication and integrity. The mentioned protocol which is a family of cluster based protocol uses Message Authentication Code (MAC) to provide authentication and integrity as well. The founders of it designed Asymmetric Pre-distribution (AP) key management scheme which sets up the shared key between neighbors in the cluster. In this protocol, there are two types of nodes, L-Sensor which includes majority of nodes in the network and H-Sensors which are the cluster heads and responsible of data aggregation and transmission to base. They also design *two-tier* routing scheme that consists of two parts: inter-cluster and intra-cluster routing. Intra-cluster routing deals with the transmission of data from L-Sensors to the cluster head (H-Sensor). To accomplish this goal, the sender sends its ID and encrypted data as well as the MAC of these two to its parent. This packet will be authenticated in the parent node through the MAC. The receiver node (the parent of sender) will send the packet to its parent and also send acknowledgment to the original sender. If the original sender does not receive an acknowledgment retransmit the packets to its parent again. In case of another failure, it selects another neighbor within the cluster and transmits the packet to it. This process continued until packet reach to destination (cluster head). The data will be stored on cluster head and after data aggregation; it will be compressed and sent to the base through the cluster head backbone (inter-cluster routing). This protocol is secure against Sybil, sinkhole, wormhole and selective forwarding attacks.

Kausar et al. proposed Key Management and Secure Routing in Heterogeneous Sensor Networks. The mentioned protocol is a family of cluster based protocol. They proposed the key management scheme based on random key distribution for heterogeneous sensor networks. This scheme significantly decreases the required space for saving the keys as it only stores one key in the sensors in comparison to random pre-key distribution. There are two types of node in this protocol: H-sensors and L-sensors. H-sensors are the ones that act as the cluster head. Therefore there are two routing schemes: inter-cluster and intra-cluster schemes. The former is deals with transmission of packets thought the cluster head backbone through the selected nodes called Relay Cells and the later is responsible for exchanging data from cluster member (L-node) to cluster head. This protocol applies Message Authentication Code (MAC) and symmetric cryptography to provide confidentiality, integrity and authentication. It also applies acknowledgment scheme to detect a selective forward attack. The idea of this scheme is very simple; if a sender node does not hear any acknowledgment from the destined neighbor in certain period of time, it will re-transmit packet to another neighbor. The mentioned protocol shows as strong resilience against node capture as the key management scheme generates the pair-wise keys between the cluster head and cluster member randomly. Finally this protocol is secure against various kinds of attack such as Sybil (which attacker select multiple identity of itself) as it applies authentication mechanism, wormhole (which attacker transmit the traffic of one place in the network to the other place through the tunnel) and sinkhole (which attacker announce the short path to sink to attract the packets and will drop them) as inter-routing uses Relay Cells and attacker could not able to participate in this routing.

Madria & Yin propose a secure routing protocol against wormhole attack (SeRWA) which not only detects the attack, but also defense against it. SeRWA is a kind of tree base routing protocol which nodes could not be moved after deployment, builds the secure path against wormhole attack without applying any specific hardware. It uses per-wise key establishment to share key between neighbors and assumed that the channel between sensor nodes are reliable thought the MAC. There are four major phases in SeRWA. *One-hop neighbor discovery* is first phase and deals with building a neighbors list for each node. When each node creates its own list exchange it with its neighbors. In this situation, nodes can detect some case of wormhole attack. Let A and B are neighbors with S_A and S_B which are the neighbor count of node A and node B respectively. According to Madria & Yin proven if $|(S_A - S_B) \text{ union } (S_B - S_A)| <= Threshold$ (they define threshold of closeness among nodes as the reverse of density of sensor network) then A and B are *Close* (distance between them is less than specific amount) or they connected through the wormhole. So in order to defense against the wormhole attack, node A and all of its neighbors reconstruct their neighbor list by omitting of nodes A, B and all neighbors of these two nodes from their list. The second

phase in SeRWA is *initial route discovery*. In this phase sink broadcast beacon and each node which receives it, mark sink (or sender) as the parent and rebroadcast it again. This process recursively continued until topology of the network will be created. *Data Dissemination and wormhole detection* is the third phase in SeRWA. In this phase, source signs the packet and send it to destination. Destination verifies the packet and sends acknowledgment. During this phase, if node finds that data packet is lost or is being modified, it will understand the wormhole attack is occurring. Therefore the nodes will reconstruct their neighbors list and omit suspicious nodes (and their neighbors as well). After detection of wormhole attack during the data dissemination, base starts the new routing request which has the same process as the second phase. This new routing is done in the *secure route discovery against wormhole attack* phase.

Lee and Choi propose SeRINS(a Secure Alternate path routing in WSN) which is a type of tree base routing protocol aiming at detection and isolation nodes which intend to inject wrong routing information from entire network. In SeRINS, there is one powerful sink (can be extended to multiple sinks) and tremendous low-power and restricted sensor nodes in which sink has an ability to have a direct communication to all nodes. Base will be authenticated via pre loaded hash value of the sensor node as follow: before deployment key pool had been generated with the rule that says the i-th key is the hash of (i+1)-th key element in the pool and the n-th (the maximum number of key in key pool) is determined randomly. After the generation of key pool, node will loaded via K_0. In order for base to be authenticated via nodes, base broadcast the value of K_1 to the nodes. Then nodes compute the hash value of K_1 and see whether it is equal to K_0 or not. If they are equal base is authenticated and they replace the value of K_0 with K_1. At the next round base will be authenticated via broadcasting of the value of K_2 and process will be continued until K_n. In this protocol, every node has multiple parents in tree, and selects one of them for forwarding the message. They use *Neighbor Report System*, to detect and delete malicious compromised nodes which try to inject inconsistence routing information in the network. The idea of this system is like this; when a node receives suspicious routing information from its neighbor, it suddenly report to base. Then base asks the neighbors of the suspicious node to announce the information about this node in the network. Sink collects the votes from the neighbors of suspicious node and determines node is really been compromised or the reporter is a compromised nod? And finally sink, omits the suspicious node from the network by revocation of its key. In this protocol, it had been assumed that a compromised node cannot broadcast inconsistent routing information to its neighbors.

Yin and Madria proposed Secure Routing Protocol for Sensor Networks (SecRout) to have secure network against compromised nodes which try to drop or modify the messages. SecRout is a family of cluster-base routing and applies two-level architecture which divided network to set of cluster with the cluster head and uses a secure and powerful sink as well. There are two types of key in SecRout. First which is shared among the nodes in the cluster is called cluster key and second is master key which is shared among the sink and cluster heads. The founders of SecRout consider four features for it. First the size of routing and data packet is very small. Second, it creates secure route and then forward packet through it and not broadcast the packet and so it has a very small amount of overhead. Third, as it mentioned before, it applies two-level architecture which data first is collect in the cluster head (through the sensor nodes which exist in the cluster) and then will be forwarded to sink. And finally it uses symmetric cryptography. All messages will be verified in SecRout through MAC. SecRout not only will detect if intimidate node drop the packets or modified them, but also detect the malicious source node which sent abnormal packet to sink.

Zhang et al. proposed A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management (RLEACH). This protocol which is a family of cluster-based protocol can be thought as security extension of LEACH. The founders of RLEACH developed a key management scheme based on random pairwise key management (RPK). The problem basic RPK scheme is that it is not adaptable to LEACH as it is not providing shared key for all nodes. In order to address this problem they proposed improve RPK key management scheme. RLEACH is resistance against the different attacks such as selective forwarding as all nodes had been integrated with the share key and attacker need to capture many nodes to achieve its objective, Sybil as it applies node to node authentication through the improved key management scheme and hello flood attack as every node need to have a permission to join the network.

Ruan et al. proposed a secure routing protocol for clustered sensor networks. The mentioned protocol is based on centralized energy-efficient routing protocol which was introduced by Maruganathan et al. in (49). In this protocol which is a family of clustered base protocol, there are one powerful base and thousands of limited sensor nodes which can act in sensor and cluster-head modes. And it is assumed that cluster head has the ability of direct communication with each cluster member and nodes cannot move after deployment as well. The founders of this protocol apply Elliptic Curve Digital Signature for message authentication to provide resistance against node compromising and perform rekeying operation periodically in order to decrease the opportunity of breaking the key for attacker. The key management scheme starts with creation of public-private key at base and assigning them, randomly, to the cluster heads through the pre-loaded shared key. Then cluster heads do the same thing to the cluster members. This protocol periodically changes the cluster head so it performs rekeying opera-

tion as it mentioned, and provides reliable route the base which make it secure against the attacks such as wormhole and selective forwarding.

Srinath et al. proposed the Authentication Confidentiality (AC) cluster based secure routing protocol for wireless sensor network. AC, which is the family of cluster routing protocol, has three layers in which the one layer has the responsibility of cluster head election, another is responsible for authentication and confidentiality and the last one deal with routing as well. The mentioned protocol, also periodically changes the cluster heads in order to decrease the chance of finding key for attackers. Additionally in this protocol, every node has a pre loaded unique identifier and certificate. For AC to work, first Cluster head broad casts its ID to the network and then nodes will send theirs ID and Certificate. After that cluster head verify the node through the certificate. Once the node is verified by cluster head, it can send data. The same process will happen for communication between cluster head and the base but, in this case data will be authentication using signature. According to the founders of AC acclaim, AC should only use when the secrecy of data is more important than the energy consumption and this maybe is drawback of this protocol.

Lan et al. proposed certainty-based secure routing protocol (CBSRP) for wireless sensor networks. CBSRP which is a family of cluster-based routing protocol applies AES cryptography to provide data secrecy and authentication mechanism. In this protocol the size of the key can be changed from 6 to 64 bits. It also uses a random function for generation of node's key. Therefore by changing the length of the key, it can fine the security level in the sensor network.

7 Security Analysis

In order to generalize previous findings, base on discussion in Section 6, the following matrix which is shown as Table 3 is presented. In the proposed matrix, secure hierarchal routing protocols in wireless sensor network are shown. It also identifies basic security requirements in wireless sensor network and specifies which protocol addresses which basic security requirements. We also try to extract the key management technique of the selected protocols and specify the cryptographic scheme. Additionally the authentication mechanism is identified for specific protocol.

TABLE 3
SECURITY MATRIX

		Protocol Name	Cryptography Scheme	Key Management Scheme	Authentication Scheme	Basic Security Requirements			
						Confidentiality	Integrity	Availability	Authentication
Secure Hierarchal Routing Protocols	1	HSRBH [40]	Symmetric Cryptography – RC4		MAC		X		X
	2	TTSR [41]	Symmetric Cryptography – RC4	Asymmetric Pre-distribution	MAC	X	X		X
	3	Key Management and Secure Routing in Heterogeneous Sensor Networks [42]	Symmetric Cryptography, Application Specific	Improved Random key distribution	MAC		X		X
	4	SeRAW [32]	Symmetric Cryptography – RC5	Pre-Distribution Key Management	It is assumed that channel are reliable through MAC		X		X
	5	SeRINS [26]	Symmetric Cryptography	Random Pre-Distribution Key Management	ARMS, MAC	X	X		X
	6	SecRout [43]	Symmetric Cryptography – RC5	The Scheme introduced in LEAP[44]	MAC		X		X
	7	RLEACH [45]		Improved Random pair-wise key management (IRPK)	Authentication is achieved via IRPK		X		X
	8	secure routing protocol for clustered sensor networks [46]	Elliptic Curves Cryptography	Public Key and Key pre-distributed schemes	Elliptic Curves Digital Signature		X		X
	9	AC [47]	Asymmetric and Symmetric Cryptography		Certificate, Signature	X	X		X
	10	CBSRP [33]	Symmetric Cryptography, AES	Random Function for key Generation	AES	X			X

According to the proposed matrix, authentication and integrity are the most satisfied security requirements among selected protocols. Therefore those protocols which addressed these requirements can resist under the attacks such as sinkhole, Sybil, selective forwarding and spoof, alter or replay routing information as they authenticate source and check for integrity of the packets. Confidentiality is placed in the third place after authentication and integrity. Those protocols which apply cryptography in order to provide data secrecy can resist against the passive attacks which attacker has the intent of monitoring the traffic in the network. It also considerable that all of selected protocols, if apply cryptography, use symmetric cryptography which is more desirable than asymmetric one due to the limitations in WSNs. We also try to identify which protocols defeat or mitigate the routing attacks which are presented previously in Section 5.2. Table 4 shows that certain protocol defeats or mitigate the effect of which routing attacks.

TABLE 4
RESISTANCE AGAINST THE ROUTING ATTACKS FOR SELECTED PROTOCOLS

	Protocol Number	Routing Attacks in WSNs					
		Wormhole	Sybil	Selective Forwarding	Sinkhole	Hello flood	Spoofed, Altered…
Secure Hierarchal Routing Protocols	1		+	+	×		+
	2	+	×	×	×		+
	3		×	+	×		
	4	×	+	+	+		+
	5		+	+	×	×	×
	6		+	×	+		×
	7		×	×	+	×	+
	8		+	×	×		+
	9		+		+		+
	10		+		+		

Note that we use different symbols in order to fill up the Table 5. Symbol '×' means that protocol defeat the certain attack as it claim via authors and '+' symbol means that protocol mitigates the effect of attack base on our pre-evaluation. If the criteria of best secure hierarchal routing protocol election be resistance against the attacks, protocols number 5 (SeRINS) and number 2 (TTSR) will be selected as the most secure hierarchal routing protocols in wireless sensor networks as they are resistance against more routing attacks.

According to the discussion in the Section 5.1, we matched these protocols to the appropriate application domain which is mentioned in Section 2. The result is presented in Table 5.

TABLE 5
PROPOSING THE SECURE HIERARCHAL ROUTING PROTOCOL IN WSNS TO APPROPRIATE APPLICATION

Application	*Basic Security Requirements*				*Appropriate Protocols*
	Confidentiality	Integrity	Authentication	Availability	
Environmental		×	×		1,3,4,6,7 and 8
Industrial		×	×		1,3,4,6,7 and 8
Healthcare	×	×	×	×	Enhancement of 2,5 and 9
Security/Critical	×	×	×	×	Enhancement of 2,5 and 9

As it shown in Table 5, which is extended of Table 1, protocols number 1, 3, 4, 6, 7 and 8 are more suitable for environmental and industrial applications as they address integrity and authentication which are the minimum security requirements for environmental and industrial application. Protocols number 2, 5 and 9 are more suitable for healthcare applications as they address authentication, integrity and confidentiality. The candidate protocols for security applications are protocol 2, 5 and 9 but as they are not addressing availability they need some enhancement to grantee all basic security requirement will be addressed.

In this section, we generalize previous findings regarding of secure hierarchal routing protocols in wireless sensor network and extracts their features such as key management schemes. Then we focus of routing attacks and identify which protocol, will mitigate or resistance against the which routing attacks. And finally base on discussion presented in Section 5.1 we proposed appropriate application for selected protocols.

8 CONCLUSION AND FUTURE WORKS

We briefly introduced wireless sensor network, its application and most wildly used elements in WSN which is sensor device. Then routing in wireless sensor networks was discussed. Additionally we reviewed some on concepts and issues concerns with security in WSN. In Section 6, selected approaches about secure hierarchal routing protocols in wireless sensor networks were represented. In the next section, we generalized previous researches about secure multipath routing protocols in WSNs and proposed a matrix in this concern. The proposed matrix may be considered as the basis for the researchers who want to work on the secure hierarchal routing protocol in wireless sensor network. And after that we identify resistance of protocols against the routing attacks and propose them for appropriate applications. In the future we intend to evaluate these protocols under variety of routing attacks and verify them to the proposed applications and utilized them with availability which has been not addressed yet.

REFERENCES

[1] Rosenberg, Aravind Iyer, Sunil S. Kulkarni, Vivek Mhatre, Catherine P. A Taxonomy-based Approach to Design of Large-scale Sensor network. s.l. : Springer, 2008.

[2] Verdone, Roberto, et al. Wireless Sensor and Actuator Networks. s.l. : Elsevier/Academic Press, 2008.

[3] Acs, Gergely ´ and Butty´an, Levente. A Taxonomy of Routing Protocols for Wireless Sensor Networks. 2007.

[4] BOUKERCHE, AZZEDINE, TURGUT, MOHAMMAD Z. AHMAD and DAMLA and TURGUT, BEGUMHAN. A TAXONOMY OF ROUTING PROTOCOLS IN SENSOR NETWORKS. Algorithm and Protocols for Wireless Sensor Networks. s.l. : Wiley, 2009.

[5] Zia, Tanveer and Zomaya, Albert Y. Security Issues and Countermeasures in Wireless Sensor Networks. Algorithms and protocols for wireless sensor networks. s.l. : John Wiley & Sons, Inc., 2009.

[6] Security of Wireless Sensor Networks. Rehana, Jinat. 2009. Seminar on Internetworking.

[7] Sensor Network Security: A Survey. Chen, Xiangqian, et al. 2009, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 11, pp. 52-73.

[8] Wireless Sensor Network Security: A Survey. Paul Walters, John, et al. 2006, Security in Distributed, Grid, and Pervasive Computing.

[9] Designing secure sensor networks . Shi, Elaine and Perrig, Adrian. 2004, IEEE Wireless Communications, pp. 38-43.

[10] A multipath routing protocol for wireless sensor network for mine security monitoring. Shuo, Xiao, Xueye, Wei and Yu, Wang. 2009, pp. 148 -151.

[11] The research and design of routing protocols of wireless sensor network in coal mine data acquisition. Guo, Yongling, et al. s.l. : IEEE, 2007. Information Acquisition ICIA '07. pp. 25 - 28.

[12] Wireless Sensor Network Based Coal Mine Wireless and Integrated Security Monitoring Information System. Yang, Wei and Huang, Ying. s.l. : IEEE, 2007. Sixth International Conference on Networking (ICN'07). pp. 13 - 13.

[13] Bauge, Tim. Wireless Sensor Networks. s.l. : THALES RESEARCH AND TECHNOLOGY (UK), 2009.

[14] A Novel Biometrics Method to Secure Wireless Body Area Sensor Networks for Telemedicine and M-Health. Poon, Carmen C. Y., Zhang, Yuan-Ting and Bao, Shu-Di. 2006, IEEE Communications Magazine, pp. 73-81.

[15] Data Privacy Considerations in Intensive Care Grids. Luna, Jesus, et al. 2008. HealthGrid.
[16] Wireless sensor networks for personal health monitoring: Issues and an implementation. Milenkovic, Aleksandar, Otto, Chris and Jovanov, Emil. 2006, The International Journal for the Computer and Telecommunications Industry, pp. 2521-2533.
[17] Elderly persons' perception and acceptance of using wireless sensor networks to assist healthcare. Steele, Robert, et al. 2009, international journal of medical informatics, pp. 788-801.
[18] Article in Press: Wireless sensor networks for healthcare: A survey. Alemdar, Hande and Ersoy, Cem. 2010, The International Journal of Computer and Telecommunications Networking.
[19] Enabling secure service discovery in mobile healthcare enterprise networks. Toninelli, Alessandra, Montanari, Rebecca and Corradi, Antonio. 2009, IEEE Wireless Communications, pp. 24-32.
[20] Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture in wireless heterogeneous networks . Huang, Y. M., et al. 2009, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, pp. 400-411.
[21] Security and privacy for mobile electronic health monitoring and recording systems. Barnickel, Johannes, Karahan, Hakan and Meyer, Ulrike. s.l. : IEEE, 2010. 2010 IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM). pp. 1 - 6 .
[22] Securing the communications of home health care systems based on RFID sensor networks. Tounsi, Wiem, et al. s.l. : IEEE, 2010. Communication Networks and Services Research Conference (CNSR). pp. 284 - 291.
[23] Securing wireless sensor networks: Security architecture. Boyle, David and Newe, Thomas. 2008, JOURNAL OF NETWORKS, VOL. 3, NO. 1, pp. 65-77.
[24] A survey on secure multipath routing protocols in WSNs. Stavrou, Eliana and Pitsillides, Andreas. 2010, Computer Networks: The International Journal of Computer and Telecommunications Networking, pp. 2215-2238.
[25] Defense Advanced Research Projects Agency. s.l. : DARPA, http://www.darpa.mil/index.html, 2008.
[26] A Secure althernate path routing in sensor netwroks. Lee, Suk-Bok and Choi, Yoon-Hwa. 2006, ScienceDirect computer communication, pp. 153-165.
[27] Secure Routing in Wireless Sensor Network: Attacks adn Countermeasures. Karlof, Chris and Wanger, David. 2003, IEEE, pp. 113-127.
[28] Sabbah, Eric and Kang, Kyoung-Don. Security in Wireless Sensor Networks. Guide to Wireless Sensor Networks. s.l. : Springer, 2009, pp. 491-512.
[29] A Survey of Security Issues in Wireless Sensor Networks. Wang, Yong, Attebury, Garhan and Ramamurthy, Byrav. 2006, IEEE Communications Surveys and Tutorials.
[30] Kizza, J.M. A Guide to Computer Network Security. s.l. : Springer, 2009.
[31] On Communication Security inWireless Ad-Hoc Sensor Networks. Slijepcevic, Sasha, et al. 2002. Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises. pp. 139 - 144 .
[32] SeRWA: A secure routing protocol against wormhole attack. Madria, Senjay and Yin, Jian. 2009, Ad Hoc Networks 7, pp. 1051-1063.
[33] The Research on Certainty-Based Secure Routing Protocol in Wireless Sensor Networks. Lan, Yoa, et al. 2006. pp. 1-5.
[34] Secure Multipath routing protocol in wireless sensor network; A security survey analysis. Modirkhazeni, Ali, Ithnin, Norafida and Ibrahim, Ousman. Alor Setar : IEEE Explore, 2010. 2th international conference on network applications, protocols and services.
[35] Daemen, Joan and Rijmen, Vincent. AES Proposal: Rijndael. s.l. : submitted to NIST as a candidate for the AES, 1998.
[36] Rivest, Ronald L. The RC5 Encryption Algorithm . 1995.
[37] Rivest, Ronald L., et al. The RC6 Block Cipher. s.l. : submitted to NIST as a candidate for the AES, 1998.
[38] New Block Encryption Algorithm MISTY. Matsui, Mitsuru. s.l. : Springer, 1997. Fast Software Encryption Workshop. pp. 54-68.
[39] Fast authenticated key establishment protocols for self-organizing sensor networks. Huang, Q., et al. s.l. : ACM Press, 2003. 2nd ACM international conference on Wireless sensor networks and applications. pp. 141-150.
[40] Scalable session key construction protocol for wireless sensor networks. Lai, Bocheng, Kim, Sungha and Verbauwhede, Ingrid. 2002. IEEE workshop on Large Scale RealTime and Embedded Systems LARTES.
[41] PIKE: peer intermediaries for key establishment in sensor networks. Chan, Haowen and Perrig, A. Pittsburgh : s.n., 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. pp. 524 - 535.
[42] Random key predistribution schemes for sensor network. Chan, Haowen, Perrig, A. and Song, D. 2003. 2003 Symposium on Security and Privacy. pp. 197 - 213 .
[43] A Key-Management Scheme for Distributed Sensor Network. Eschenauer, Laurent and Gligor, Virgil D. Washington : s.n., 2002. The 9th ACM conference on computer and communication security. pp. 41-47.
[44] Perfectly-secure key distribution for dynamic conferences. Blundo, Carlo, et al. s.l. : Springer, 1992. 12th annual international cryptology conference on advances in cryptology. pp. 471-486.
[45] Theory and application of cryptographic techniques. Blom, R. Berlin : Springer, 1985. Eurocrypt 84 workshop on advances in cryptology. pp. 335–338.
[46] Lee, Jooyoung and Stinson, Douglas R. Deterministic Key Predistribution Schemes for Distributed Sensor Networks. Selected Areas in Cryptography. s.l. : Springer, 2005, pp. 294-307.
[47] Gura, Nils, et al. Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs. 2004.
[48] TinySec: A Link Layer Security Architecture for Wireless Sensor Networks. Karlof, Chris, Sastry, Naveen and Wagner, David. 2004. Second ACM conference on embedded networked sensor systems (SensSys 2004). pp. 162–175.
[49] Detecting Wormhole Attacks in Wireless Sensor Networks with Statistical Analysis. Zhao, Zhibin, et al. s.l. : IEEE, 2010. WASE International Conference on Information Engineering. pp. 251 - 254.
[50] An Approach towards Detection of Wormhole Attack in Sensor Networks. Prasannajit B, Venkatesh, et al. 2010. WASE International Conference on Information Engineering. pp. 283 - 389.
[51] Secure Routing in Wireless Sensor Network: Attacks and Countermeasures. Karlof, Chris and Wanger, David. 2003, IEEE, pp. 113-127.
[52] LITEWORP: A lightweight countermeasure for wormhole attack in multihop wireless networks. Khalil, Issa, Bagchi, Saurabh and Shroff, Ness B. s.l. : IEEE, 2005. International conference on depandable systems and networks. pp. 1 - 10.
[53] A secure routing protocol for ad hoc networks. Sanzgiri, Kimaya, et al. 2002. 10th IEEE International Conference on . pp. 78 - 87 .
[54] Graaf, Rennie de, et al. Distributed Detection of Wormhole Attacks in Wireless Sensor Networks. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. s.l. : Springer, 2010, pp. 208-223.
[55] Defending against wormhole attacks in mobile ad hoc networks. Wang, Weichao, et al. 2006, Wireless Communications & Mobile Computing.
[56] Using Directional Antennas to Prevent Wormhole Attacks. Hu, Lingxuan and Evans, David. 2004. Network and Distributed System Security Symposium (NDSS).
[57] Secure and resilient clock synchronization in wireless sensor networks. Sun, Kun, Ning, Peng and Wang, Cliff. 2006, IEEE Journal on Selected Areas in Communications, pp. 395 - 408 .
[58] Secure neighbor discovery in wireless networks: formal investigation of possibility. Poturalski, Marcin, Papadimitratos, Panos and Hubaux, Jean-Pierre. New York : ACM, 2008. 2008 ACM

symposium on Information, computer and communications security .

[59] Secure neighborhood discovery: a fundamental element for mobile ad hoc networking. Papadimitratos, P., et al. 2008, IEEE Communications Magazine, pp. 132 - 139 .

[60] Butty´an, Levente, D´ora, L´aszl´o and Vajda, Istv´an. Statistical Wormhole Detection in Sensor Networks. Authenticated Queries in Sensor Networks, Lecture Notes in Computer Science. s.l. : Springer, 2005, pp. 128 - 141.

[61] An approach to mitigate wormhole attack in wireless ad hoc network. Lee, Gunhee, Kim, Dong-kyoo and Seo, Jungtaek. 2008. International conference on information security and assurance. pp. 220 - 225.

[62] Cha, Woosuck, Wang, Gicheol and Cho, Gihwan. A Pair-Wise Key Agreement Scheme in Ad Hoc Networks . Lecture Notes in Computer Science. s.l. : Springer, 2004.

[63] Krawczyk, H., Bellare, M. and Canetti, R. HMAC: Keyed-Hashing for Message Authentication, RFC 2014. 1997.

[64] An innovative approach for wormhole attack detection and prevention in wireless sensor networks. Azer, Marianne A., El-Kassas, Sherif M. and El-Soudani, Magdy S. s.l. : IEEE , 2010. International conference on Networking, Sensing and Control (ICNSC). pp. 366 - 371.

[65] Rogers, Everett M. Diffusion of Innovations. s.l. : Free Press, 1996.

[66] Ad-hoc on-demand distance vector routing. Perkins, Charles E. and Royer, Elizabeth M. 1999. Second IEEE workshop on Mobile Computing Systems and Applications. pp. 90 - 100.

[67] Detection of wormhole attack in multipath routed wireless ad hoc networks; statistical analysis approach. Qian, Lijun, Song, Ning and Li, Xiangfanf. s.l. : Journal of Network and Computer Applications, 2007, Vol. 30.

[68] Mobile Sink Using Multiple Channels to Defend Against Wormhole Attacks in Wireless Sensor Networks. Rasheed, Amar and Mahapatra, Rabi. Scottsdale, AZ : IEEE Explorer, 2009. 2009 IEEE 28th International Performance Computing and Communications Conference (IPCCC) . pp. 216 - 222.

[69] Establishing pairwise keys in distributed sensor networks. Liu, Donggang and Ning, Peng. 2003. 10th ACM conference on Computer and communications security . pp. 52 - 61.

[70] Bronshtein, Ilja, et al. Handbook of Mathematics. s.l. : Springer, 2007.

[71] Analysis of Public-Key Cryptography for Wireless Sensor Networks Security. Amin, F., Jahangir, A. H. and Rasifard, H. s.l. : World Academy of Science, 2008, World Academy of Science, Engineering and Technology 41, pp. 529 - 534.

[72] Sabbah, Eric and Kang, Kyoung-Don. Security in Wireless Sensor Networks. Guide to Wireless Sensor Networks. s.l. : Springer, 2009, pp. 491-512.

[73] A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks . Poovendran, Radha and Lazos, Loukas. 2007, Wireless Networks, pp. 27-59.

[74] Investigation of feasible cryptographic algorithms for wireless sensor network. Choi, Kyung Jun and Song, Jong-In. 2006. Advanced Communication Technology, 2006. ICACT 2006. pp. 1379-1381.

[75] Cho, Young-Geun, Kang, Jeonil and Nyang, DaeHun. Proactive Code Verification Protocol in Wireless Sensor Network. Lecture Notes in Computer Science. s.l. : Springer, 2007, pp. 1085–1096.

[76] Empirical Study on Secure Routing Protocols in Wireless Sensor Networks. Modirkhazeni, Ali, Ithning, Norafida and Ibrahim, Othman. 5, s.l. : IJACT : International Journal of Advancements in Computing Technology, 2010, Vol. 2, pp. 25 - 41.

[77] A Centerilzed Energy-Efficient Routing Protocol for Wireless Sensor Networks. Muruganathan, S. D., et al. 2005, IEEE Communication Magazine Vol 43.

[78] LEAP: Efficient Security Mechanisms for Larg-Scale Distributed Sensor Networks. Zhu, S, Setia, S and Jajodia, S. Washing : s.n., 2003. ACM Conference on Computer and Communication Security.

[79] Verdonel, Roberto, et al. Wireless Sensor and Actuator Networks. 2008.