Academic Journal of Nawroz University (AJNU), Vol.10, No.4, 2021

https://doi.org/10.25007/ajnu.v10n4a957

A Systematical Roadmap on Various Security Vulnerabilities and Countermeasures in Routing Algorithms upon WSNs

Idrees S. Kocher

Department of Energy Engineering, Technical College of Engineering, Duhok Polytechnic University, Duhok, Kurdistan Region-F.R. Iraq.

ABSTRACT

Wireless Sensor Networks (WSN) is now an evolving technology and has a broad range of applications, such as battlefield surveillance, traffic surveillance, detection of forest fires, detection of floods, etc. The communication nature of the wireless sensor network is unprotected and dangerous due to deployment in hostile environments, restricted resources, an automatic nature, and untrusted media for broadcast transmission. For wireless sensor networks, several routing protocols have been suggested, but none of them have been developed with protection as a target. The majority function in routing algorithms currently in place for sensor networks optimize a restricted capacities in sensor nodes and the application based design of WSNs. A WSNs, however, are exposed to a number of possible threats that impede the network's regular activity. Thus, there is a strong need to provide the routing protocols of the OSI structure layer with a safe mechanism to prevent an attacker from obstructing it. The well-known attacks against all layers are discussed in this systematic roadmap, and debilitating attacks against routing protocols are analyzed and defined in particular. Several suggested attack countermeasures, design considerations and paper contributions are also included in the routing protocols. The assertion of the study is that WSN routing protocols must be built with protection in mind, and this is the only efficient solution in WSNs for safe routing. The aim of this paper is also to provide problems, attacks and countermeasures related to protection. Finally, it is hoped that this roadmap would inspire potential researchers to come up with smarter and better protection measures and make their network safer. The first such research analysis of secure routing protocols in WSNs is this roadmap study.

KEYWORDS: Attacks, vulnerability, countermeasures, OSI, wireless sensor network, secure routing protocols.

1. Introduction

The deployment in an unattended setting of sensor nodes renders the WSNs vulnerable. In military, environmental, health and commercial applications, WSNs are being used increasingly. For the acceptance and use of sensor networks, WSN protection is essential. In particular, unless there is complete proof of protection for the network, the WSN product in the industry will not be approved (Vaishali and Sharda, 2015). The dispersal of WSNs into the territory of an opponent allows the identification of opponent`s equipment in the military climate.

Home based sensor systems have the capability to monitor the aged health and to identify intrusions in home settings via a home automation surveillance system. Lives of millions will depend on the timely delivery and reliability in both of these circumstances of the sensing data collected from scattered sensors within entire WSNs. Consequently, to deter an attacker from preventing the provision of legitimate sensed data or copying the sensed data, certain sensor network must always be protected.

For the identification of fabricated sensor information, the end-to-end proper cryptography functions combined with post processing of sensed message are helpful to overcome a mentioned problem (Hu et al., 2003a; Ye et al., 2004; Estrin et al., 1999).

This roadmap study considers recent proposals for routing protocols in WSNs optimize the unique design of the networks for restricted capacities of WSN components and for underlying application as well, but do not consider security. Although these protocols have not been developed with safety as a target, it is necessary to examine their protection

properties in this review. For weak wireless channel, restricted capacities of sensor nodes, potential insider attacks and the opponents may depend on powerful high-energy smart devices and long-range communication to assault the network, it is non-trivial to design a demanded secure routing algorithms. This systematical roadmap presents debilitating attacks against all the major routing protocols. Since these protocols have not been developed as a target for defense, it is unsurprising that they are all dangerous. This is not easy to address, however, it is impossible that a sensor network routing protocol will be made safer by adding authentication mechanisms after completion of the architecture. Our assertion is that protocols for sensor network routing must be built with protection in mind, and this is the only effective approach for WSNs safe and secure routing.

This systematical roadmap is organized as follows. Various inherently resources constrained upon WSNs are debated in section 2. In Section 3, various security necessities upon WSNs are provided. Section 4 presents a possible security attacks types upon WSNs. Proposed countermeasures (defenses) on DoSs attacks are introduced in section 5. Section 6 provides some proposed secure algorithms for WSNs. Finally, the conclusions, paper contribution, comparative table of well-known secure routing protocols and their countermeasures to well-known attacks on WSNs and many trends for the future some future research activities are debated in section7.

2. INHERENTLY RESOURCES CONSTRAINED IN WSNs

This network consists of a vast number of fundamentally resource constrained sensor devices. The processing capacity of these nodes is small, the storage capacity is very low and restricted bandwidth for communication. Such constraints are due to the sensor nodes' insufficient resources and physical dimensions. The shortcomings of WSNs that are well known are considered and listed below:

- **Unattended Environmental Networks.** In most situations, in distant areas, sensor nodes in a WSN are installed and left unattended. Therefore, the risk of sensor pruning to physical attack may be great. Using distant control for WSNs applications leads to physical tampering that almost difficult to detect (Idrees et al., 2013).
- **Power restrictions.** Power seems to be the greatest restriction of WSNs. The study shows each transmitted bit in WSNs absorbs around as much consumed energy as 900 instructions are executed as done by (Hill et al., 2000). Therefore, in WSNs, communication is more expensive than computation. Furthermore, applying complicated security scheme for securing WSNs almost contributes to deplete resource energy of the nodes very soon (Idrees and Qusay, 2016).
- **Restricted Memory Storage.** A sensor node is a compact computer with just a limited amount of storage space and memory. After loading the OS, there is no longer sufficient storage to work with large size algorithms (Idrees, 2020). The 16 bit, 8-MHz central processing unit holding 10-Kbyte RAM, 48-Kbyte program memory and 1024 - Kbyte flash storage for typical sensor type TelosB. Therefore, the latest protection algorithms are unfeasible for these sensors.
- **Unreliable contact techniques.** The broadcasting communication via radio waves is another real threat against sensor protection. Because of channel failures, packets can get destroyed or may get lost at heavily congested nodes. Higher

error rates often involve the introduction of rigorous error handling systems that result in higher overhead. And if the channel is correct, the contact cannot be so under some situations. Due to the telecast associated with wireless networking, the packets that overlap in transmission and there is strong need to resend them later. In general, the transparent design of the wireless medium is necessarily less protected and hence increased vulnerability to different kinds of wireless media malicious attacks (Vaishali and Sharda, 2015)

- **Increased communication latency.** Higher message delivery latency can result from multi-hop based routings, network traffic overcrowding and intermediate sensor node operation.

  Such delay can make it very difficult to handle sy nchronization management in WSNs (Vaishali and Sharda, 2015).

3. SECURITY NECESSITIES IN WSNS

Security services in WSNs can secure the data exchanged across the network and the infrastructure from sensor node attacks and wrongdoing. Here are the most significant protection necessities in WSNs:

- **Authentication Process.** This guarantees that the transmitting sensor is the one it appears to be for destination node. Not only can an attacker alter data packets, but it can also alter the stream of message via inserting faked messages. Therefore, the recipient node needs providing the Message Authentication Code (MAC) scheme to verify that the packets received actually came from the sender node (Wood et al., 2002).
- **Confidentiality of payload.** The authentication function must provide guarantee for integrity that no content is recognized by someone other than the authorized destination node within WSNs. The following conditions should be discussed in a WSNs secrecy process (Idrees and Qusay, 2016; Idrees and Qusay, 2017):
  a) The main structure for delivery should be highly stable.
  b) A sensor node does not permit neighbors to access its readings unless they are allowed to do so.
  c) In some circumstances, publicly available metadata like sensor names and shared secure sensor node keys could also be encoded which defend against transit analyst attackers.
- **Method of data integrity.** This mechanism can guarantee that an object does not change any message when it traverses from the source to the destination (Vaishali and Sharda, 2015).
- **Process for Data freshness.** This presumes that perhaps the content is new and guarantees that an opponent will not reproduce old messages. For verifying the message freshness of WSNs, a time based counter or the nonce have to be applied and attached to every message (Vaishali and Sharda, 2015).
- **Phase of self-organization.** In a WSNs, it is important for each sensor node to have been self-organized and self-healed. This functionality also presents a significant challenge to work. The hierarchical design of WSNs makes it almost impossible for the nodes and the BS to launch some preinstalled shared key feature. Not only about multi-hop routing, or for secure key management process and confidence relationships to be carried out, it is important that the sensor nodes inside a WSNs have the capability of personality organize themselves

(Vaishali and Sharda, 2015; Eschenauer et al., 2002).

- **Stable localization process.** It is important to locate all sensor nodes in a WSNs correctly and automatically in many cases. The WSNs functionality is to find possible faults, for example, will need specific sensor node position to classify the existing faults (Capkun et al., 2006; Vaishali and Sharda, 2015).
- **Synchronization process.** The majority of sensor network applications need time synchronization. It is also important to time-synchronize the protection mechanism for WSNs. Synchronization between groups of sensor nodes may be needed for a collaborative WSNs (Ganeriwal et al., 2005; Vaishali and Sharda, 2015).
- **Method of availability.** These requirements mean that, even in the case of internally or externally threats including a DoSs threats, WSN facilities can still be used (Idrees et al., 2011; Vaishali and Sharda, 2015).

4. SECURITY ATTACKS TYPES IN WSNs

The Open Systems Interconnection (OSI) architecture model is followed by the most popular WSN architecture. Five layers and three cross-layers are part of the WSN architecture. It mostly needs five layers, namely application, transport, n/w, data link & physical layer. This study provides the features of various attacks types upon OSI structure in WSNs in the following subsections.

4.1 Denial of Services (DoSs) Attacks

It is characterized as an event that decreases or attempts to decrease the ability of a network to perform its anticipated operation. In the literature, there are some typical methods (approaches) to deal with some of the more common attacks issued by DoSs attacks. In the following paragraphs, the most famous DoSs attacks are presented in details (Wood et al., 2002).

4.2. Attacks on Transport layer

In general, the transport layer is susceptible to the two forms of attacks described in the following brief subtypes:

- **Method of Flooding.** Even when a method (protocol) is needed at either end of a connection to preserve the state, it is vulnerable to memory exhaustion due to floods attacks (Wood et al., 2002). The new link requests can be made repeatedly by the attacker until the resources needed by each connection is depleted or exceeds the full limit. In any case, there will be additional legal requests would be missed due to attacker activity.
- **De-synchronization.** It refers to a current link connection being disrupted by attacker (Wood et al., 2002). For example, an attacker may constantly spoof messages to the end host, forcing the host to order the missing frames to be retransmitted. If properly occurred, an attacker can weaken or block the recipient's capacity from sharing information effectively, exhausting their resources rather, and recovering from faults that really never occur.

4.3. Attacks on Network Layer

In general, the network layer is susceptible to the various forms of attacks described in the following brief subtypes:

- **Hello flood attack.** In general, many protocols using hello packets make it easy to conclude that getting this message ensures such transmitter is within receiver's broadcast range. To trick most of sensors to think that their locations are still within their neighborhood, an intruder can use a

high-powered transmitter. Consequently, the intruder sensor node wrongly spreads a shorter path to the BS then tries to relay all recipient of hello packets to the fake node where all are now no longer within the attacker's range (Karlof et al., 2003).

- **Sinkhole Attack.** with such a threat, by modifying the routing information, an attacker can make a corrupted sensor node appear most appealing to its neighbors. This outcome is that now the adjacent nodes pick the infected node to route as its next-hop node (Karlof et al., 2003).
- **Wormhole Attack.** The wormhole attack is known to be a low delay link between two connected devices by which an attacker replays network messaging. The intruder gathers packets then pipes them to some other place in the network where the messages are sent back into the network. This relationship can be formed either by exchanging messages via a single sensor node between two next but still no contiguous sensors, or by connecting to each other via a two sensor nodes in separate sections of the network (Karlof et al., 2003).
- **Spoofing Attack.** The routing information for WSNs is attacked by this type to interrupt network traffic control. To interrupt network traffic control, an attacker can fake, change, and repeat routing data. This involves the development of loops for underlying root, the attraction or repulsion of traffic control to or from chosen sensor nodes, the extension or shortening of sending routes, the production of false error signals, the rise in end-to - end latency and the partitioning of the network (Karlof et al., 2003).
- **Selective forwarding attack.** All sensor nodes in WSNs have to correctly start sending right communicated messages. In a somewhat way that it deliberately forwards certain messages and dropping another, an attacker can corrupt a sensor node.
- **Sybil or Multi-Identities Attack.** One sensor node in a WSN introduces many identities for this attack. It was initially presented as a threat attempted to overcome the target of replication mechanisms in peer-to - peer networks in decentralized data storage systems. It's also very efficient against routing algorithms, aggregation of data, polling, equal distribution of resources, and detection of corruption thwarting (Newsome et al., 2004).
- **Blackhole and Grayhole Threat.** Under path discovering phase with proactive routing protocols or under route upgrade packets with reactive routing algorithms, a Blackhole attack, depicted as just a hostile sensor node, wrongly publicizes the fastest or most effective route to intended sensor node. A hostile node's purpose may be to obstruct the process of discovering the route or to locate all the packet data sent to the appropriate sink node. Whilst the grayhole attack is a more subtle form of blackhole threat, here hostile sensor node loses the packet data temporarily, this leads to make it even harder to identify.
- The hostile node's purpose may be to obstruct the process of discovering the route or to locate all the packet data sent to the appropriate sink node.
- **Byzantine Attack.**A tampered sensor node or a group of malicious node operates in conspiracy to perform this attack which aim to launch harms such as build in loops, sending messages on ineffective paths, and falling packets deliberately.

It is quite harder to detect this form of attack, because WSN normally does not show any irregular behavior under such attack (Awerbuch et al., 2002).

- **Information Disclosure Attack.** An infected sensor node can disclose sensitive or substantial data to unauthorized sensor nodes in the WSNs in this attack. This information often include records related to the topology of the network, the geographical position of nodes, or the best routes of WSNs to approved sensor nodes.
- **Resource Depletion Attack.** Such as battery capacity, bandwidth, and processing power are the usual assets threatened by this attack. In the form of very regular creation of beacon packets, unwanted requests for paths, and routing of stale packets to other nodes, a hostile sensor node attempts to drain resources of other nodes in WSNs.
- **Acknowledgment Spoofing Attack.** Certain network protocols in WSNs demand the delivery of packets of acknowledgement. Intruder will probably hear packet packets from the neighboring nodes and fake the acknowledgments, supplying the sensor nodes inside entire WSNs with false details**.**

4.4. Attacks on Link layer

Some drawbacks such as collisions, resource exhaustion and allocation unfairness were generated by attacks on this layer. A collision happens as two sensor nodes try to simultaneously transmit at a same frequency. They are thrown away when packets clash and have to be retransmitted. Through particular packets such as Acknowledge "ACK" control packets, an intruder may tactically cause collisions. In an effort to create collisions, the intruder may easily breach the network communication and transmit messages repetitively. A weak form of DoS attack is extremely unfair. For this scenario, the opponent tends to cause real-time applications going to run on other sensor nodes to deteriorate entire WSNs (Wood et al., 2002).

4.5. Attacks on Physical Layer

Under aggressive or vulnerable locations, where an intruder has full access, the sensor nodes in WSNs can be deployed. Two sorts of threats occur in the physical layer in general:

- **Tampering Attack.** The sensor nodes are particularly vulnerable to physical attacks due to their unsupervised and scattered existence. Unavoidable disruption to the nodes can be caused by physical attacks. The opponent will steal the caught node's cryptographic keys, tamper with its hardware, change program codes, or even substitute them with a deceptive sensor.
- **Jamming Attack.** This is a form of attack that tries to interfere with the frequency bands used for connectivity by the sensor nodes in WSNs. To interrupt the whole network, a jamming source might be strong enough. Also with fewer effective sources of jamming, by selectively scattering the jamming sources, an attacker will effectively interrupt connectivity in the whole network Syeda et AL., 2018.

4.6 Attacks on Privacy and Authentication

This roadmap analysis provides several types of attacks that can be released under such a classification:

- **Privacy Attack:** The protection of privacy in WSNs is often more difficult than the conventional networks because these networks find it possible to reach vast amounts of data via

remote monitoring systems. Because the intruder doesn't have to be directly available to carry out the monitoring, with a relatively low risk, the data collecting process may be performed secretly. Moreover, remote access allows several locations to have been tracked concurrently by a sole opponent. As seen below, this roadmap addresses some very well-known privacy attacks:

a) **Eavesdropping.** Any attacker could quickly understand the contents whenever the messages are not secured by cryptographic techniques. Packets holding WSN control messages transmit more data than can be retrieved from the servers. Spying on such packets proves to be more efficient for such an opponent.

b) **Traffic Analysis.** In order to establish a successful threat on privacy, the eavesdropping mechanism can be coupled with traffic analysis. By means of an effective traffic analysis, anadversary can identify certain sensors with particular routines in a WSN. Any massive rise in the exchange of messages between certain sensor nodes, for example, means that these sensor nodes have certain particular behaviors and events to track.

c) **Camouflage:** only after sensor node has been infected by the opponent in the WSNs and then used by that sensor node to disguise the usual sensor devices in the network. When the messages begin to appear at the infected sensor node, they begin to be routed to strategic sensor nodes where they can regularly carry out privacy review upon this messages**.**

- **Node Cloning Attack.** There, the intruder wants to connect a sensor node to a current WSN by cloning the sensor node identity of a network node that already exists. Throughout this way, the sensor node copied and attached to the network may effectively cause serious interruption in WSN data transmission by corrupting and forwarding the packets on incorrect paths. It can also contribute to segmentation of the network, transmission of false readings of sensors etc.

5. PROPOSED COUNTERMEASURES (DEFENSES) ON DOS ATTACKS

This systematical roadmap focuses on how to protect data in transport and network layers of OSI structure in WSNs. Thus this section provides some well-known attacks and their corresponding countermeasures on DoSs attacks on transport and network layers as discussed in the following subsections.

In general, several possible DoSs attacks on OSI structure of WSNs with their corresponding countermeasures are introduced as in Table 1.

5.1. Proposed Countermeasures on Transport Layer DoSs Attacks

This section provides some DoSs well-known attacks which can be initiated on transport layer and their corresponding countermeasures as discussed in the following subsections:

- **Flooding DoSs Attacks.** The analysis of this roadmap proposes applying the strategy that use client puzzles to protect against flooding DoSs threats as done in (Idrees, 2011b; Idrees, 2016; Aura et al., 2001). A key concept is that by solving the puzzle, each linking client can show its contribution to the connection. It would be difficult for an attacker to build links quickly

sufficient to induce energy depletion at working sensor node, since an intruder most definitely would not have unlimited resources.

- **De-synchronization attack.** It's really able to secure against the transport layer's de-synchronization threat through introducing the compulsory authentication mechanism for those messages exchanged across sensors devices. When indeed the checking function works in a reliable way, any faked messaging cannot be sent via an intruder (Idrees, 2011b; Idrees, 2016; Wood et al., 2002).

5.2. Proposed Countermeasures on Network Layer DoSs Attacks

The following attacks and their countermeasures which can be conducted on the network layer are given in this section:

- **Selective Forwarding Attack.** Selective forwarding attack can be defended in several ways, like using multiple routes to send information, identifying the suspicious sensor node, and deciding that it has missed and finding an alternative path for the next stage.
- **Spoofing and alteration attack.** To combat spoofing and alteration messaging in WSNs, there is a strong need to attach Message Authentication Code (MAC) within sending packet. The receiver will check the integrity of packet contents with the help of this attached MAC field.

TABLE 1: The Possible DoSs Attacks on OSI Structure of WSNs and Their Corresponding Countermeasures

OSI WSN Layer Names	Possible Threats	Countermeasures Methods	Countermeasures Methods Refs.
Transport	Flooding	Client Puzzles	{Wood et al., 2002; Idrees, 2011b; Idrees, 2016}
	De-synchronization	Authentication	{Wood et al., 2002; Idrees, 2011b }
Network	Hello Flood	{Authentication, Packet Leashes, Implementing Temporal and Geographic Data}	{Zhan et AL.,2010; Idrees, 2011b; Idrees, 2016; Karlof et al., 2003}
	{Selective Forwarding Spoofing and Alteration Attacks}	{Egress filtering, Authentication and Monitoring}	{Karlof et al., 2003}
	Replayed Attack	counters or time-stamps	{Idrees, 2011b; Idrees,2016}
	Wormhole Attacks	{Idrees, 2011b; Idrees,2016},Authentication and Probing	{Karlof et al., 2003}
	Blackhole Attack	Enhanced path-finding	{Deng et al., 2002a}
	Grayholes Attack	Isolate hostile node	{Sen et al, 2007b}
	Sinkhole	Redundancy Check	{Karlof et al., 2003; Idrees, 2011b; Idrees,2016}
	Sybil	{Redundancy Check, Authentication and Monitoring}	{Newsome et AL., 2004}
	Acknowledgement Flooding	{Authentication, Bidirectional Link Authentication Verification}	{Karlof et al., 2003; Idrees, 2011b; Idrees,2016}
Link	Exhaustion	Rate Limitation	{Wood et al., 2002}
	Collision	Error Correction Code (ECC)	{Wood et al., 2002}
	Unfairness	Small Frames	{Wood et al., 2002}
Physical	Jamming	Priority messages, Spread Spectrum, Low Duty Cycle and Mode Change	{ Syeda et AL., 2018}

- **Replayed Attack.** To protect against this form of attack, almost a time-stamps or counter device are inserted in packets.

- **Wormhole Attacks.** This analysis indicates that the following methods should be used to protect against this particular attack:
  a) Through implementing a smart antenna strategy to monitor wormhole attacks as done in (Hu et al., 2004a).
  b) Through introducing a new and generic technique called packet leashes, as done in (Hu et al., 2004b), to identify then protect against wormhole attacks.
  c) This theory suggests that perhaps an attacker node sensor overhears on such a sequence of packets, then tunnels and replays them along a network. This will be achieved in order to create the distance between two conspiring nodes a false perception. Most commonly, it's used to interrupt the routing mechanism through confusing the discovery mechanism of neighbors (Karlof and Wagner, 2003).
  d) Uses the visualization technique, as done in (Wang et al., 2004b), to find wormholes in WSNs. The distance measurement is performed among all neighborhood`s sensor nodes within entire WSNs in this reference. In this context, the graphical configuration for entire network is calculated using multi-dimensional scaling with the help of surface smoothing technique for modifying a round off failures. Eventually, it analyzes the outline of the resultant virtual network. A network structure will bent and curl into the wormhole whenever the wormhole occurs, else the system will appear flat.
- **Blackhole Attack:** Writers have suggested the strategy to define and detach a single blackhole node (Ashfaq and Farrukh, 2012;Deng et al., 2002a). However, the security hazard emanating from the condition in which multiple blackhole sensors function under combination has not really been addressed. With specifics, refer to the reference above.
- **Grayholes Attack:** In this approach, they suggested secure protocol that would detect cooperative grayhole attacks. Grayhole identification is perhaps more complicated than blackhole identification, because these nodes temporarily lose packets and frequently change the behavior in order to prevent tracking. For a single node, or for a large number of nodes, the effect of grayhole activity can be seen. As in suggested method, each node in the grid gathers then retains data transmission information for its neighborhood in Data Routing Information (DRI) table. Recall for functionality details refer to above reference (Sen et al, 2007b).

6. SOME PROPOSED SECURE ALGORITHMS FOR WSNs

This systematical roadmap study suggests some secure algorithms for securing the WSNs as discussed in the following subsections.

6.1. Secure Broadcast Authentication Algorithms

The broadcast authentication proposed technique for the SPINS algorithm (Perrig et al., 2002) is the micro variant (µTESLA). The above µTESLA implements asymmetry by delaying a reveal of symmetric keys, resulted through an successful authentication system by broadcasting. This needs the BS and the sensor nodes to have been closely coordinated for its service. Furthermore, each node should consider a maximal correlation fault of an upper limit. The call for feature specifics relates to the relation listed above.

6.2. Secure Multicasting and Broadcasting Algorithms for WSNs

A right protective system must be implemented

WSNs to guarantee that certain approved recipient members can agree to receive packets treated under this category of communication. Numerous key management systems have indeed been developed to deal with this problem:

- Centralized group key management protocols: In order to retain the group nodes of WSNs, a central authority is managed.
- Decentralized key management protocols: This procedure is to split the group management activity among group of sensor devices at this model.
- Key Management Distributed System: Instead of using one sensor node, this management mechanism is spread amongst groups of sensor nodes. The entire sensor nodes are liable for management role of this scheme for particular WSNs.

In general, using a logical key tree framework is an easy way to assign keys in a WSN. These approaches fall into the heading of main control algorithms that are clustered. However centralized methods are not often the most effective, while these methods can often be very effective for WSNs, since in effective BS, comparatively heavier calculations can typically be done.

Multicast method adopted directed diffusion approach for WSNs uses the hierarchy of logical key as has been suggested by writers (Di Pietro et al., 2003). A main key provider has been in tree root of logical hierarchy while the all sensor nodes are within branches. All internal tree's sensor nodes hold keys used during the re-keying phase.

In (Lazos and Poovendran, 2003), the authors suggested a method by creating the hierarchy of logical key for the purpose of providing secure multicast link. All nodes are clustered into various clusters on the basis of geographical location knowledge. Through a single hop contact, the nodes inside a cluster are able to reach each other. A key hierarchy is built by using cluster data in a manner close to that suggested in (Lazos and Poovendran, 2002).

7. Conclusions and Future Works

7.1. Conclusions

The adoption and use of WSNs is useful for many applications creating a safe routing, but this roadmap has demonstrated that recent routing protocols in the literature for these networks are vulnerable and insecure. A cryptography in Connection layer and authentication methods can be a fair first indication for defensive measure anti sensor class outsiders, still cryptographic system will not be enough defensive measure against laptop class opponents and insiders. So, the purpose of this paper presented and suggested concerns, threats and defensive measures related to security. Eventually, there's also a clear need for cautious implementation of security routing algorithm to overcome the listed below concerns:

1) The choice of suitable cryptographic techniques relay on the capability of the nodes of the network. A protection protocols, however, are extremely application specific.

2) Sensors were distinguished by energy constraints, computing power, memory, and bandwidth of communications. These restrictions must be satisfied by the architecture of security services in WSNs.

3) Sensor networks mobility has a significant effect on the topology of the network and hence poses many problems in secure routing protocols, once considered as a fixed situation for most current approaches.

7.2. Paper Contributions

The following suggested contributions are given in

this systematic roadmap study:

i. For secure routing in WSNs, it recommends hazard models and security priorities.
ii. This study describes different potential attacks on WSNs' OSI structure layers.
iii. This study implements different defense mechanisms to address a very well-known routing threats in WSNs.
iv. Eventually, this would enable potential developers to keep coming up with more intelligent and reliable protection measures to make their network secure.t literature approaches.

7.3. Comparative Table of Well-Known Secure Routing Protocols and Their Countermeasures to Well-Known Attacks on WSNs

As seen in Table 2, this roadmap analysis presented a comparative table of well-known secure routing protocols and their countermeasures to well-known attacks on WSNs.

7.4. Many Trends for the Future

In the field of WSNs security study, some potential developments are defined as follows:

- **Quality of Service (QoSs) as well as protection.** Latest research on protection in WSNs concentrate on specific field including key control, safe routing, safe data collection and intruders prevention. For WSNs, quality of service together with defense have to be measured jointly.
- Promote a functionality of sensor nodes with private key activities.
- Promote the secure routing algorithm solution for mobile WSNs.
- Improving the challenges with time synchronization.
- Creation of broadcast authentication methods in high scalability including effectiveness.

TABLE 2: A Comparative Table of Well-Known Secure Routing Protocols and Their Countermeasures to Well-Known Attacks on WSNs

Algorithm Ref.	Idrees,011b Idrees,016 TamperSec	LKHW Di Pietro,'03	SecLEACH Han,'10	KeyChain Liu, '03	LEAP Zhu,'04b	SecRoute Sen, '10	SIGF Wood,'06	TARF Zhan,'10	RLEACH Zhan,'08	SPINS Perrig,'02
Threats	Pecho,'09									
Hello Flood	√		√	√	√	√	√	√	√	√
Eavesdropping	√	√	√		√	√	√	√	√	√
Rout Poisoning	√	√	√	√		√	√		√	√
Sinkhole	√		√		√	√	√	√	√	√
Blackhole	√		√		√	√	√	√	√	√
Grayhole	√		√		√	√	√	√	√	√
Wormhole	√		√					√	√	√
Sybill	√				√	√	√	√	√	√
Replay	√	√	√	√	√	√	√		√	√
Devic Replication	√	√	√			√				√
Device Impersonation	√	√			√	√		√		√

8. REFERENCES

1. Farooqi A.H. & Khan F.A. (2012),"A survey of Intrusion Detection Systems for Wireless Sensor". Int. J. Ad Hoc and Ubiquitous Computing, 9 (2), 69-83.

2. Vaishali P. & Sharda K. (2015),"Attacks and Challenges in Wireless Sensor Network. IJESRT, 4(6), 122-130, June 2015.

3. Idrees S. K. & Qusay I. S. (2017)."Classifying Routing Algorithms upon Clustered Based Wireless Sensor Networks: A Survey". ZANCO Journal of Pure and Applied Science (ZJPAS), 29(2), 25-36 , Salahaddin University, Erbil, Iraq, **2017**.

4. Aura T. Nikander P. & Leiwo J. (2001). DoS-resistant authentication with client puzzles. Proceedings of the 8th International Workshop on Security Protocols, 170-177, Springer-Verlag, Germany.

5. Deng H., Li H. & Agrawal D. (2002a). Routing security in wireless ad hoc networks. IEEE Communications Magazine, 40(10).

6. Deng J.,Han R. & Mishra S. (2004). Countermeasures against traffic analysis in wireless sensor networks. Technical Report : CU-CS-987-04, University of Colorado at Boulder.

7. Di P. R., Mancini L.V. , Law Y.W. , Etalle S. & Havinga P. (2003). LKHW : a direced diffusion-based secure multi-cast scheme for wireless sensor networks. Proceedings of the 32nd International Conference on Parallel Processing Workshops (ICPPW'03), pp. 397-406, IEEE Computer Society Press, 2003.

8. Syeda G. F., Syed A. S. & Mohammed S. (2018), Efficient Defense System for Jamming Attacks in

Wireless Sensor Networks. International Journal of Electronics and Communication Engineering and Technology, 9(4), 2018, 22–35.

9. Estrin, D. ; Govindan, R. ; Heidemann, J.S. & Kumar. S. (1999). Next century challenges: scalable coordination in sensor networks. Mobile Computing and Networking, 263-270.

10. Eschenauer, L. & Gligor, V.D. (2002). A key-management scheme for distributed sensor networks. Proceedings of the 9th ACM Conference on Computer and Networking, 41-47.

11. Ganeriwal, S. ; Capkun, S. ; Han, C.-C. & Srivastava, M.B. (2005). Secure time synchronization service for sensor networks. Proceedings of the 4th ACM Workshop on Wireless Security, 97 – 106, New York, USA, ACM Press.

12. Han, Y-J. ; Park, M-W. & Chung, T-M. (2010). SecDEACH : secure and resilient dynamic clustering protocol preserving data privacy in WSNs. Proceedings of the International Conference on Computational Science and its Applications (ICCSA'10), 142 – 157,
13. Hill, J. ; Szewczyk, R. ; Woo, A. ; Hollar, S. ; Culler, D.E. & Pister, K. (2000). System architecture directions for networked sensors. Proceedings of the 9th International Conference on Architectural Support for Programming Languages and Operating Systems, 93-104, ACM Press.
14. Hu, L. & Evans, D. (2003a). Secure aggregation for wireless sensor networks. Proceedings of the Symposium on Applications and the Internet Workshops, p. 384, IEEE Comp. Soc. Press.
15. Hu, L. & Evans, D. (2004a). Using directional antennas to prevent wormhole attacks. Proceedings of the 11th Annual Network and Distributed System Security Symposium.
16. Hu, Y. ; Perrig, A. & Johnson, D.B. (2003b). Rushing attacks and defense in wireless ad hoc network routing protocols. Proceedings of the ACM Workshop on Wireless Security, 30 – 40, 2003.
17. Hu, Y. ; Perrig, A. & Johnson, D.B. (2004b). Packet leashes: a defense against worm-hole attacks. Proceedings of the 11th Annual Network and Distributed System Security Symposium.
18. Karlof, C. & Wagner, D. (2003). Secure routing in wireless sensor networks : attacks and countermeasures. Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, 113-127.
19. Lazos, L. & Poovendran, R. (2002). Secure broadcast in energy-aware wireless sensor networks. Proceedings of the IEEE International Symposium on Advances in Wireless Communications (ISWC'02).
20. Lazos, L. & Poovendran, R. (2005). SERLOC : robust localization for wireless sensor networks. ACM Transactions on Sensor Networks, 1 (1), 73 -100.
21. Lazos, L. & Poovendran, R. (2003). Energy-aware secure multi-cast communication in adhoc networks using geographic location information. Proceedings of the IEEE International Conference on Acoustics Speech and Signal Processing.
22. Liu, D. & Ning, P. (2003). Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks. Proceedings of the 10th Annual Network and Distributed System Security Symposium, 263 – 273, San Diego, CA, USA.
23. Liu, D. & Ning, P. (2004). Multilevel µTESLA: broadcast authentication for distributed sensor networks. ACM Transactions on Embedded Computing Systems (ECS), 3(4), 800-836.
24. Newsome, J.; Shi, E. ; Song, D. & Perrig, A. (2004). The Sybil attack in sensor networks: analysis and defenses. Proceedings of the 3rd International Symposium on Information
25. Processing in Sensor Networks, 259-268, ACM Press.

26. Pecho, P.; Nagy, J.; Hanacke, P. & Drahansky, M. (2009). Secure collection tree protocol for tamper-resistant wireless sensors. Communications in Computer and Information Science, Vol. 58, 217 – 224, Springer-Verlag, Heidelberg, Germany.
27. Perrig, A. ; Szewczyk, R. ; Wen, V. ; Culler, D.E. & Tygar, J.D. (2002). SPINS: security protocols for sensor networks. Wireless Networks, 8(5), 521-534.
28. Perrig, A. ; Stankovic, J. & Wagner, D. (2004). Security in wireless sensor networks. Communications of the ACM, Vol. 47, No. 6, pp. 53 – 57.
29. Sen, J ; Chandra, M.G. ; Harihara, S.G. ; Reddy, H. & Balamuralidhar, P. (2007b). A mechanism for detection of grayhole attack in mobile ad hoc networks. Proceedings of the 6th International Conference on Information, Communication, and Signal Processing (ICICS'07), 1 – 5, Singapore.
30. Sen, J. & Ukil, A. (2010). A secure routing protocol for wireless sensor networks. Proceedings of the International Conference on Computational Sciences and its Applications (ICCSA'10), 277 – 290, Fukuaka, Japan.
31. Wang, W. & Bhargava, B. (2004b). Visualization of wormholes in sensor networks. Proceedings of the 2004 ACM Workshop on Wireless Security, 51 – 60, New York, USA, ACM Press.
32. Wood, A.D. & Stankvic, J.A. (2002). Denial of service in sensor networks. IEEE Computer, 3510), 54-62.

33. Zhu, S. ; Setia, S. & Jajodia, S. (2004b). LEAP : efficient security mechanism for large-scale distributed sensor networks. Proceedings of the 10th ACM Conference on Computer and Communications Security, 62 – 72, New York, USA, ACM Press.
34. Zhang, K. ; Wang, C. & Wang, C. (2008). A secure routing protocol for cluster-based wireless sensor networks using group key management. Proceedings of the 4th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM'08), 1-5,
35. Zhan, G.; Shi, W. & Deng, J. (2010). TARF: a trust-aware routing framework for wireless sensor networks. Proceedings of the 7th European Conference on Wireless Sensor Networks (EWSN'10), 65 – 80, Coimbra, Portugal.
36. Idrees S. K. (2020). Software Engineering Methods To Improve The Design Of Software Reliability Systems: Roadmap. Journal Of Southwest Jiaotong University 55 (3), 1-9, June 2020, DOI : 10.35741/issn.0258-2724.55.3.27, **2020.**
37. Idrees G. & Qusay I. S. (2016) "Performance Evaluation of Novel Secure Key Management Scheme Over BAN Wireless Sensor Networks". Journal of University of Duhok, 19(1) (Pure and Eng. Sciences), 179-188, **2016**.
38. Idrees S. G., Chee-On C., Tanveer A. Z. & Qusay I. G. (**2011a**) Cross-layer based security solutions for wireless sensor networks, International Journal of the Physical Sciences (IJPS), 2011, 6(17), 4245-4254, **2011.**
39. Idrees S. G., Chee-On C., Tanveer A. Z. & Qusay I. G. (**2011b**). A Novel Secure Key Management Module for Hierarchical Clustering Wireless Sensor Networks, 3rd International Conference on Computational Intelligence, Modeling and Simulation (CIMSim 2011). Langkawi, Malaysia**.2011.**
40. Idrees S. K., Chee-Onn C., Hiroshi I., & Tanveer A. Z. (**2013**). Threat Models and Security Issues in Wireless Sensor Networks, International Journal of Computer Theory and Engineering, 5(5), 830-835.