TAF Journal of Advances in Technology and Engineering Studies JATER
2017, **3**(1): 27-36

PRIMARY RESEARCH

A comprehensive comparison and classification of routing attacks in wireless sensor networks

Ahmed A. Mohsin *

Supervision and Scientific Evaluation Directorate, Ministry of Higher Education and Scientific Research, Baghdad, Iraq

Index Terms
Wireless Sensor Network (WSN)
Network Layer
Security
Routing
Attacks

Received: 21 September 2016
Accepted: 25 October 2016
Published: 12 February 2017

***Abstract*—** Security has become a primary concern not only for researchers, but also for many users. Wireless Sensor Networks (WSNs) are susceptible to various kinds of attacks, so the need to protect such networks has been increased. There are a number of challenges in WSN security design. Resource constraints such as the ability of processing, low battery life, small memory size and unsecured transmissions make various attacks more dangerous for these networks. Our attention of this paper concentrates on the most typical routing attacks and their capabilities which influence network layer. The attackers can potentially compromise one or more of security goals of the network they attack. This paper is expressing a comparison between routing attacks to find the purpose of the attackers on WSNs' functionality. It classifies and compares them extensively based on different features such as goals, the threat nature, attack function, WSNs' threat site and according to disruption of the route or consumption of the resources. This paper also gives a better understanding of future direction for researchers for designing secure WSNs.

I. INTRODUCTION

Wireless sensor network (WSN) is designed to check and communicate with other devices over a specific geographic area and control physical environments from remote locations. Today's WSN is used widely in various applications, including Surveillance, environmental monitoring and many others. WSNs are networks formed by many smart, small, energy constrained, self-organizing and low-cost devices [1]. Sensor networks can deal with different applications and run in unfriendly and uncontrolled environments. However, due to the size of sensor nodes, sensor energy restrictions, changes of the sensor network topology, lack of global identification in sensor nodes and type of tasks expected from the sensors, WSNs' security faces challenges and issues in employing any efficient security scheme different from traditional network security [2]. In section 2, the major design challenges in WSN security are explored. Section 3 reviews the goals of WSN's security. In Sections 4, various types of attacks against network layer are categorized. The classification and comparison of routing attacks about network layer in section 5 are outlined. Finally, section 6 points out the conclusion of the research.

A. Design Challenges of WSN Security

In WSNs, the understanding of security challenges provides a basis for further works on sensor network's security. WSNs suffer from many design challenges such as resource limitations of sensor nodes and using of insecure communication channels. Various attacks are likely to succeed due to the limited resources available to mitigate the attacks [1] [3] [4] and [5]. For example, Zigbex sensor type HBE has an 8-bit, 7.372 MHz ATmega128L RISC MCU with only 4 Kb SRAM, 128 Kb flash memories and 512 Kb flash storage [6]. With such Very Limited Resources, the software built for the sensor node must also be quite small. The process by security schemes should be selected based on the following criteria:

*Corresponding author: Ahmed A. Mohsin
†Email: frederick_patacsil@yahoo.co.uk

A. Power consumption: how much power is required to execute the encryption decryption functions? When implementing a cryptographic function within a sensor node, each computation and transmission of message consume power. Further, the power consumption of sensor nodes is increased due to the security function processing that is required (e.g., encryption, decryption). Each type of encryption/decryption algorithm affects the power consumption at different settings for each algorithm. These settings include different sizes of data blocks and key size.
B. Program memory: the memory required to store the encryption/decryption program. One of the requirements to implement security scheme is to have enough memory space to run security algorithm after loading OS and application code. Moreover, the program memory indicates how much more storage has to be used by the sensor node, which also decreases power.
C. Execution time: the time required to execute the encryption/decryption code. Each cryptographic program has a special execution time which can be measured. The more extra time a sensor node has to be active, the more power is consumed.
D. Program Parameters memory: the required memory size to save the required number of keys used by the encryption/decryption function. Under these criteria, it is important to think about the security requirements very carefully to implement a secure cryptographic algorithm in wireless sensor networks. Applying any security scheme requires transmission of extra bits, hence extra processing, memory and battery power, which are very important resources for the sensors' long life. Table 1 presents various cryptographic algorithms comparison for different parameters like code requirement and cost (time/energy) from [7].

TABLE 1
COMPARISON OF CRYPTOGRAPHIC ALGORITHMS FOR CODE AND COST REQUIREMENTS

Encryption	Decryption	Cost (time/energy)	Code requirements
RSA	RSA	3.8 s	13387B (512 bit key)
RC5	RC5 (Block)	Variable (No. of neighbors)	ROM: 17.9KB RAM: no. of neighbors
CTR mode	RC5 (Block)	7.24 ms	2674B
CBC mode (Optional)	Cipher independent	RC5(C, assembly):0.26ms	RAM: 728B program space: 7146B

B. Security Goals of WSNs

Implementing security into WSNs is impossible to implement perfectly. WSNs are susceptible to security attacks due to the broadcast nature of transmission medium and placing nodes in a hostile or dangerous environment where they are not physically protected. It is unfeasible to monitor and protect each individual sensor in a large-scale sensor network from physical or logical attack. In this section, the goals of Security in WSN are summarized in table 2 as follows [8], [9].

C. Network Layer Security Attacks

The network layer is responsible for routing and forwarding information into the network, such as routing the packets between sensor nodes and routing the packets from a node to the base station. As described earlier, WSNs are susceptible to a large diversity of attacks on the different protocol layers. Particularly, the network layer of WSNs is vulnerable to the different types of attacks that disrupt routing information, create fake routing messages, and degrade the network performance. Attacks in network layer can be classified into two major categories, namely passive and active attacks. Passive attacks are not involved in the protocol, attacker observes protocol, tries to gain information without altering it. Detection of such an attack is not easy since the data and operations of the network itself don't get affected. Active attacks mean active interference of attacker and alter of protocol or data being exchanged in the network. The attacks can also be classified into two categories, namely external attacks and internal attacks. External attacks are defined as attacks from nodes, which do not belong to a WSN; internal attacks occur when legitimate nodes of a WSN behave in unplanned ways. Hence there is need to summarize the major attacks against WSNs, most network layer attacks may be classified as one of the following attacks, as shown in Table 3 [8].

ISSN: 2414-4592
DOI: 10.20474/jater-3.1.5

TABLE 2
WSN SECURITY GOALS

Goals	Details
Confidentiality	Confidentiality means ensuring that the content of the data transmitted among sensor nodes is hidden from everyone in the networks except authorized sensor nodes. Moreover, Identities of the Sensor nodes and secure key management are extremely important by using encryption. Data should be restricted within the WSN and not reveal to the sensor nodes neighbors [10].
Integrity	Integrity refers to the ability to ensure the data have not been altered by malicious nodes sent by unauthorized parties. Attackers can alter significant data in packets. Even if the confidentiality has been measured, there is still a possibility that the integrity of data has been compromised by alterations. A cyclic redundancy checksum (CRC) and checksum are employed for detecting changes in packets.
Authentication	Authentication, make sure that the data are initiated from the claimed sender that is exact at the intended receiver. The receiver node must verify if an accepted message comes from a true sender. That is, the sender and the receiver share a public or secret key to compute the message authentication of all communicated data.
Availability	Which ensures that the desired WSN services and information are available at any time they are needed. The primarily an availability attack is a denial-of-service attack that makes the network unable to prepare service [24, 25].
Data Freshness	Data freshness ensures that the data contents are recent and fresh. This requirement is very important when there are shared key establishments employed in the design of a network that changes over time since is no fixed infrastructure among the sensor nodes and the base station in the WSN.
Secure Localization	During the implementation of security protocol, the secure localization of each sensor node automatically and accurately is an important property that must be a guarantee. WSN uses the graphical information to determine the identity of each node.
Accountability	Unique identification of the entity responsible for any requesting or sending data.
Controlled Access	The ability to access certain services or information by only authorized entities.

D. Routing Attacks' Classification

This section tried to classify and compare the routing attacks based on the nature, threat, location and the type of attack (here classification according to routing disruption attack and/or resource consumption attack is considered); as shown in following table 4, the most important known routing attacks on WSNs; this table has four columns, including security nature, attack function, WSNs' threat location and according to aiming for disruption of the route or/and consumption of the resources. Our purpose of security nature of attacks includes passive or active. Attack threat shows which security service is attacked, includes confidentiality, integrity, authenticity, availability, data freshness, secure localization, accountability and controlled access. The attacker location (insider or outsider), and based on attack's type on WSN's protocols, include disruption attack and resource consumption attack or both.

Following figure 1 shows the nature of WSN's routing attacks; it compares these attacks based on their nature by presenting the percentage ratio of routing attacks, which is based on passive or active attack; 83 percent of routing attacks' nature is active; 17 percent of routing attacks are passive.

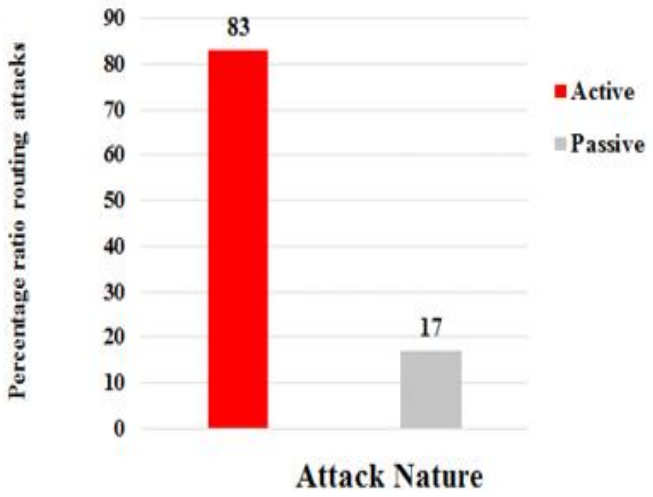

Fig. 1 . The nature of WSN's routing attack

ISSN: 2414-4592
DOI: 10.20474/jater-3.1.5

TABLE 3
ROUTING ATTACKS' DESCRIPTION

Attacks	Description
Blackhole Attack	It is a type of Denial-of-Service (DoS) attack, malicious node utilizes the routing protocol in order to advertise itself as having the shortest route to the destination node and hence source nodes select this shortest path and go through this malicious node and result in drape packets and break communications between sensor nodes [14]. As soon as the malicious node receives this routing request, it immediately responds with a false reply to the source node. It replies blindly to every routing request to convince the source node that it has the shortest path route to the destination. Therefore, the malicious node becomes source node and controls the whole traffic flows received by it.
Wormhole Attack	The wormhole attack is the most severe attack on the routing functionality of wireless networks that can affect the network even without the knowledge of cryptographic algorithms implemented. It disrupts the communications across the network and is difficult to protect against because they use a private channel, which is invisible to the WSN. A single or pair of malicious nodes may launch wormhole attack. The attacker receives packets at one location in the network, and tunnels those to another location at a distant location and retransmitting them locally into the WSN through virtual tunnels, thus creates a wormhole. Wormholes are classified into three types: closed, half open, and open.
Sybil Attack	Every actual node in the sensor network has a unique identity. In Sybil attack, an adversary pretends to be more than one node using forging multiple identities of other legitimate nodes in multiple locations at the same time by obtaining the legitimate person's IP address, MAC address or public keys [17]. Sybil attack can be performed for attacking the distributed storage, data aggregation, fair allocation of resources among the nodes, quality of services in networks and geographical and multipath routing protocols.
Selective forwarding attack	Selective forwarding attack, a special case of denial of service attack, an attack where the malicious node refuses to forward packets to certain nodes or drop packets of certain types on the route selectively ensuring they are not propagated any further [18]. In addition, the malicious node may send the packets to the wrong routing path [19], [20]. Selective forwarding attack also behaves like a Blackhole in which it drops every packet it receives. The adversary places itself on the actual data flow path between the two communicating nodes, sends a false routing information and disrupts the network operation and discards some packets.
Neglect and greed attack	Neglect and greed when packets are transferred from a source to destination in between, an attacker can force multi-hopping, drops incoming packets arbitrarily and gives undue priority to its own messages. This attack causes degradation of traffic and disturbs the network system, in which nodes may not be capable of sending or receiving packets.
Sinkhole attack	In this type of attack, the compromised node tries to place itself on the network flows as a fake base station (BS) and sends fake routing information to its neighbors to attract network traffic to itself with respect to the routing algorithm [21]. Then all the packets pass through it. The aim of an adversary is to prevent base station from acquiring a complete sensing data from nodes in the network [22]. WSNs are mainly vulnerable to sinkhole attacks. Sinkhole attack can be used to launch other series of attacks [23]. The compromised node tries to attract as much traffic as possible in the entire network [24].
HELLO flood attacks	The routing protocol consists of hello packets that transmit between sensor nodes. An attacker broadcasts hello message with strong transmission power and acts as a fake sink. The victim nodes think that the malicious node is their neighbor and go through the malicious node as this node provides the shortest path to send packets to the base station. This leads to data congestion and disturbing of the data flow in the network [25].

ISSN: 2414-4592
DOI: 10.20474/jater-3.1.5

TABLE 3 Cont'd...

Acknowledgment spoofing attack	This attack can spoof network layer Acknowledgments on routing algorithms that need transmission of acknowledgment packets. A malicious node may overhear packets' transmissions from its neighboring nodes, alter acknowledgments, thereby disseminating erroneous information about the status to the nodes of WSN.
Rushing attack	In this attack, fast broadcastings the false advertisings of route request before other nodes in the WSN. Thereby, correct request will discard, other attacks will launch and finding any usual routes will fail.
Homing attack	In this attack, Adversary monitors and analyzes the network traffic for special nodes (cluster heads, key managers) that have special responsibilities in WSN, trying to eavesdrop on their activities and gain contents of the messages [26] and [27]. Adversaries create new routing paths, lengthen or shorten the source routes, extract sensitive data and destroy the sensor node resources.
Gratuitous detour attack	In this attack, an attacker tries to detour data flow to a suboptimal route. Where a route seems legitimate by adding virtual nodes where a shorter route exists and that causes exhaustion of resources and routing loops.
Eavesdropping	Eavesdropping is detecting and analyzing of gathered information from a network by snooping on data transmitted. An attacker snoops secretly between any two nodes in network and may monitor, access and extract the sensitive information concerning connection for further cryptanalysis or traffic analysis.
Misrouting attack	Misrouting: In such attack a malicious node misroute flows away from intended destination or many flow in one direction, it is hard to detect this kind of attacks. This type of attack can lead to a Packet's misdirection, wrong routing path and reducing the WSN's availability.
Flooding attack	Flooding attack one of various types of attacks which decreases network lifetime, the flooding is one of them. An attacker continuously propagates many connection requests to a susceptible node to prevent the node from establishing communications. The main goal of flooding attacks is to reduce availability and exhaust the resources like the memory and energy of the node in the network system.
Routing Information Alteration (spoofing)	In this attack, routing information included in the packets may be altered, spoofed or may replay routing information. These disruptions to traffic in the network include creating new path cycles, discarding routing information, generating false error messages, and exhausting resources in WSNs.
Impersonation	Impersonation attack is also called identity spoofing or node replication in which the attacker assumes the identity of one of the legitimate nodes during the communication, thus an attacker obtains confidential information. The information may include the location or keys of the node in the network.
Byzantine attack	In this attack, a single compromised node works alone or a set of compromised nodes could work in collusion, under full control of an adversary, and thus disrupts the communication of other nodes in the network. Such an attack creates routing loops, forwarding packets in suboptimal routes, or selectively dropping packets.
Traffic analysis	In a traffic analysis attack, an adversary monitors packet transmission to obtain critical information such as the identity of sources or destinations, bandwidth consumption, the location of the base stations and the type of protocols being used.
Camouflage	In camouflage attack, malicious node compromises of a sensor node in the sensor network by masquerading as normal sensor node. This camouflaged node may advertise fake routing information, misroute the packets from other node or drop the packets.
Node malfunction	An adversary can cause node malfunction and generates inaccurate data. An adversary destroys integrity, exhausts resources and degrades efficiency of WSN.
Information disclosure	This type of attack is aimed at gaining valuable information to unauthorized nodes in the network including network topology, location of nodes or optimal routes to authorized nodes. The more information that an attacker knows about a node, the easier the network will be to compromise.

ISSN: 2414-4592
DOI: 10.20474/jater-3.1.5

TABLE 3 Cont'd...

State pollution attack	This type of attack occurs when a malicious node provides incorrect reply parameters regarding request parameters and that leads to broadcasting duplication of address nodes frequently in the network.
Resource Consumption Attack	In resource consumption Attack, the attacker consumes the target network resources like the limited resource of energy, bandwidth, or memory by broadcasting Route Request packets with a different broadcast ID. The result of this attack is typically the denial of one or more services offered by the target nodes.
IP spoofing attack	IP spoofing, also known as IP address forgery, a malicious node impersonates a trusted node and occupies the same IP address in the network, the attacker gains the IP address of a legitimate node.
The Packet Replication Attack	In a packet replication attack, the attack occurs inside the network for the resource. The results are that the adversary consumes the bandwidth and the power of the network.
Sleep deprivation	It's also called Resource consumption attack, the aim of this kind of attack is to consume the resources (e.g. battery power, bandwidth, etc.) of the specific node of the network so as to minimize the lifetime of the network, by keeping them busy in routing decisions and forgo their sleep cycles, hence stop functioning. Attackers broadcasting continuously a large number of route request to the target node.
Routing table overflow	In this case, an attacker tries to create routes to non-exist nodes in the network by injecting false routing control packets to a target node and preventing new routes from being created.
Message injection attack	An attacker injects fake control information into the packets.
Message modification attack	An adversary makes some changes to the routing messages before retransmitting.
Replay attack	The adversary performs a replay attack by first intercepting valid control packets and then by resending those to make other nodes in the network update their routing tables with stale routes.

Figure 2 shows a comparison of WSNs' routing attacks based on their security threat factors including Authenticity, Availability, Data Freshness, Secure Localization, Accountability and Controlled Access, in percentage ratio; it presents 100 percent of security threats targeting secure localization, 83 percent of security threats targeting data freshness, accountability and controlled access. 27 percent of them are targeting confidentiality.

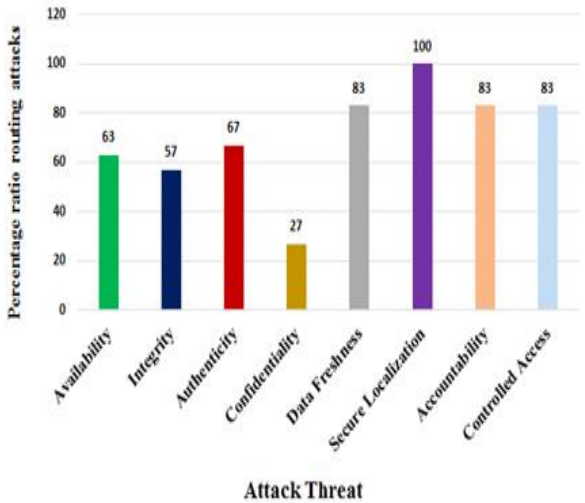

Fig. 2 . The WSN's routing attacks based on their security threats

ISSN: 2414-4592
DOI: 10.20474/jater-3.1.5

TABLE 4
ROUTING ATTACKS' CLASSIFICATION

Attack	Nature	Attack Threat	Location	Attack Type
Blackhole Attack	active	authenticity, Availability, Data Freshness, Secure Localization, Accountability, Controlled Access	Both	Both
Wormhole Attack	active	Confidentiality, authenticity, Data Freshness, Secure Localization, Accountability, Controlled Access	Both	Both
Sybil Attack	active	Availability, authenticity, integrity , Data Freshness, Secure Localization, Accountability, Controlled Access	Both	Both
Selective forwarding attack	active	Availability, integrity, Data Freshness, Secure Localization, Accountability, Controlled Access	inside	Routing Disruption
Neglect and greed attack	active	Availability, authenticity, Data Freshness, Secure Localization, Accountability, Controlled Access	inside	Routing Disruption
Sinkhole attack	active	Availability, integrity, authenticity, Data Freshness, Secure Localization, Accountability, Controlled Access	Both	Routing Disruption
HELLO flood attacks	active	Availability, authenticity, Data Freshness, Secure Localization, Accountability, Controlled Access	inside	Routing Disruption
Acknowledgement Spoofing attack	active	Integrity, authenticity, Data Freshness, Secure Localization, Accountability, Controlled Access	Both	Routing Disruption
Rushing attack	active	Availability, integrity, authenticity, Data Freshness, Secure Localization, Accountability, Controlled	Access	outside Both
Homing attack	passive	Confidentiality, Secure Localization	outside	Resource Consumption
Gratuitous detour attack	active	Availability, integrity, authenticity, Data Freshness, Secure Localization, Accountability, Controlled Access	outside	Both
Eavesdropping attack	passive	Confidentiality, Secure	Localization	outside
Misrouting attack	active	Availability, integrity, authenticity, Data Freshness, Secure Localization, Accountability, Controlled Access	outside	Both
Flooding attack	active	Availability, integrity, authenticity, Data Freshness, Secure Localization, Accountability, Controlled Access	inside	Resource Consumption
Routing Information Alteration (spoofing)	active	Integrity, authenticity, Data Freshness, Secure Localization, Accountability, Controlled Access	Both	Both
Impersonation	active	Availability, integrity, confidentiality, authenticity, Data Freshness, Secure Localization, Accountability, Controlled Access	outside	Both

ISSN: 2414-4592
DOI: 10.20474/jater-3.1.5

TABLE 4 Cont'd...

Byzantine attack	active	Availability, Integrity, authenticity, Data Freshness, Secure Localization, Accountability, Controlled Access	outside	Routing Disruption
Traffic analysis	passive	Confidentiality, Secure	Localization	outside
Camouflage passive Confidentiality, Secure Localization outside Routing Disruption Node malfunction	active	Availability, authenticity, Data Freshness, Secure Localization, Accountability, Controlled Access	outside	Resource Consumption
Information disclosure	passive	confidentiality, Secure	Localization	outside
State pollution	active	Availability, integrity, authenticity, Data Freshness, Secure Localization, Accountability, Controlled Access	Both	Routing Disruption
Resource consumption attack	active	Availability, Data Freshness, Secure Localization, Accountability, Controlled Access	Both	Resource Consumption
IP spoofing	active	Availability, integrity, confidentiality, authenticity, Data Freshness, Secure Localization, Accountability, Controlled Access	Both	Routing Disruption
The Packet Replication Attack	active	Availability, Data Freshness, Secure Localization, Accountability, Controlled Access	inside	Resource Consumption
Sleep deprivation	active	Availability, Data Freshness, Secure Localization, Accountability, Controlled	Access Both	Both
Routing table overflow	active	Availability, integrity, authenticity, Data Freshness, Secure Localization, Accountability, Controlled Access	outside	Both
Message injection	active	Integrity, authenticity, Data Freshness, Secure Localization, Accountability, Controlled Access	outside	Routing Disruption
Message modification	active	Integrity, authenticity, Data Freshness, Secure Localization, Accountability, Controlled Access	outside	Routing Disruption
Replay attack	active	Integrity, Data Freshness, Secure Localization, Accountability, Controlled Access	Both	Routing Disruption

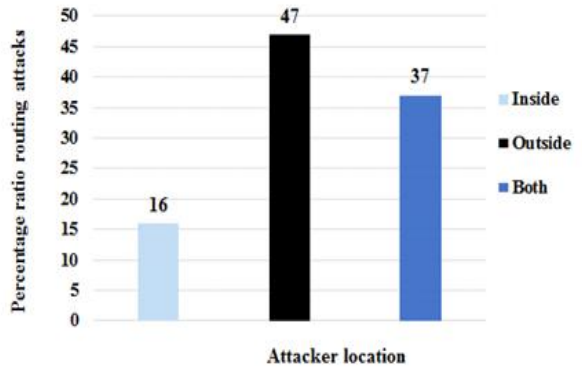

Fig. 3 . Percentage ratio of every routing attack

Figure 3 shows the percentage ratio of attacker location; it compares these attacks based on their location; as a result, the occurred percentage of WSNs' routing attacks, in attacker location, are 16 percent insider, 47 percent out of WSNs' range (outsider) and 37 percent from both.

Figure 4 shows that how much percentage ratio of every routing attack by targeting disruption of the routing or consuming the resources on WSNs. For example, almost 40 percent of these attacks are aiming to disrupt the routing of WSNs, and 17 percent of them are attacking the WSNs' resources, 33 percent of them are aiming both of those types which means to disrupt the route and consume

ISSN: 2414-4592
DOI: 10.20474/jater-3.1.5

the resources together.

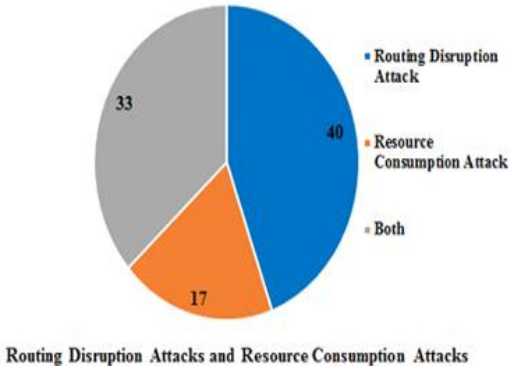

Fig. 4 . The types of WSN's attacks targeting disruption of the routing and/or consuming the resources

II. CONCLUSION

Under the limitations of WSNs, it is vital to think about the security requirements very carefully to obtain the best way for securing the transmitted data and extending WSNs in different environments. In this paper, WSN security goals are specified and then well-known routing attacks based on different dimensions are classified and compared. Comparison of classification routing attacks based on the nature, threat, site and the type of attack. The importance of introducing the purpose and classification of well-known routing attacks is to evaluate the risk potential of the attackers and compare it to the cost of protection when designing a proper secure routing protocol. Also, it's showing the effect of the attackers on the WSNs' functionality. However, I wish this comprehensive study could help to guide researchers working on the security issues in the network layer of WSNs.

REFERENCES

[1] D. G. Padmavathi and M. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," *International Journal of Computer Science and Information Security,* vol. 4, no. 1 & 2, 2009.

[2] M. A. Rahman and M. K. Debnath, "An energy-efficient data security system for wireless sensor network," in *11th International Conference on Computer and Information Technology,* 2008. **DOI:** 10.1109/iccitechn.2008.4802984

[3] M. Felamban, B. Shihada and K. Jamshaid, "Optimal node placement in underwater wireless sensor networks," in *IEEE 27th International Conference on Advanced Information Networking and Applications (AINA),* 2013. **DOI:** 10.1109/aina.2013.40

[4] S. Saleem, S. Ullah and H. S. Yoo, "On the security issues in wireless body area networks," *JDCTA,* vol. 3, no. 3, pp. 178 184, 2009. **DOI:** 10.4156/jdcta.vol3.issue3.22

[5] J. Ben-Othman and B. Yahya, "Energy efficient and QoS based routing protocol for wireless sensor networks," *Journal of Parallel and Distributed Computing,* vol. 70, no. 8, pp. 849-857, 2010. **DOI:** 10.1016/j.jpdc.2010.02.010

[6] HBE-Zigbex, "Ubiquitous sensor network," Zigbex Manual [Online]. Available: http://www.hanback.co.kr.

[7] G. Sharmaa, S. Balaa and A. Vermaa, "Security frameworks for wireless sensor networks-review," *Procedia Technology,* vol. 6, pp. 978-987, 2012. **DOI:** 10.1016/j.protcy.2012.10.119

[8] P. Mohanty, S. Panigrahi, N. Sarma and S. S. Satapathy, "Security issues in wireless sensor network data gathering protocols: A survey," *Journal of Theoretical and Applied Information Technology,* vol. 13, no. 1/2, pp. 14-27, 2010.

[9] X. Chen, K. Makki, K. Yen and N. Pissinou, "Sensor network security: A survey," *IEEE Communications Surveys & Tutorials,* vol. 11, no. 2, pp. 52-73, 2009. **DOI:** 10.1109/SURV.2009.090205

[10] K. Ren, S. Yu, W. Lou and Y. Zhang, "Multi-user broadcast authentication in wireless sensor networks," *IEEE Transactions on Vehicular Technology,* vol. 58, no. 8, pp. 4554-4564, 2009. **DOI:** 10.1109/TVT.2009.2019663

[11] L. B. Oliveira, D. F. Aranha, C. P. Gouvêa, M. Scott, D. F. Câmara, J. López and R. Dahab, "TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks," *Computer Communications,* vol. 34, no. 3, pp. 485-493, 2011. **DOI:** 10.1016/j.comcom.2010.05.013

[12] C. Gomez and J. Paradells, "Wireless home automation networks: A survey of architectures and technologies," *IEEE Communications Magazine,* vol. 48, no. 6, pp. 92-101, 2010. **DOI:** 10.1109/MCOM.2010.5473869

[13] K. Sunitha and H. Chandrakanth, "A survey on security attacks in wireless sensor network," *International Journal of Engineering Research and Applications (IJERA),* vol. 2, no. 4, pp. 1684-1691, 2012.

ISSN: 2414-4592
DOI: 10.20474/jater-3.1.5

[14] S. Tamilarasan, "Securing and preventing AODV routing protocol from black hole attack using counter algorithm," *International Journal of Engineering Research and Technology,* vol. 1, no. 5, pp. 1-5, 2012.

[15] M. A. Azer, S. M. El-Kassas and M. S. El-Soudani, "An innovative approach for the wormhole attack detection and prevention in wireless ad hoc networks," in *International Conference on Networking, Sensing and Control (ICNSC),* 2010. **DOI:** 10.1109/ICNSC.2010.5461523

[16] B. Bhargava, R. de Oliveira, Y. Zhang and N. C. Idika, "Addressing collaborative attacks and defense in ad hoc wireless networks," in *29th IEEE International Conference on Distributed Computing Systems Workshops,* 2009. **DOI:** 10.1109/icdcsw.2009.77

[17] D. N. Sushma and V. Nandal, "Security threats in wireless sensor networks," *IJCSMS International Journal of Computer Science & Management Studies,* vol. 11, no. 01, 2011.

[18] L. K. Bysani and A. K. Turuk, "A survey on selective forwarding attack in wireless sensor networks," in *International Conference on Devices and Communications (ICDeCom),* 2011. **DOI:** 10.1109/icdecom.2011.5738547

[19] W. Xin-Sheng, Z. Yong-zhao, X. Shu-ming and W. Liang-min, "Lightweight defense scheme against selective forwarding attacks in wireless sensor networks," in *IEEE International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery,* 2009. **DOI:** 10.1109/cyberc.2009.5342206

[20] K. Venkatraman, J. VijayDaniel and G. Murugaboopathi, "Various attacks in wireless sensor network: survey," *International Journal of Soft Computing and Engineering,* vol. 3, no. 1, pp. 208-211. 2013.

[21] A. Pandey and R. C. Tripathi, "A survey on wireless sensor networks security," *International Journal of Computer Applications,* vol. 3, no. 2, pp. 43-49, 2010. **DOI:** 10.5120/705-989

[22] P. Samundiswary, D. Sathian and P. Dananjayan, "Secured greedy perimeter stateless routing for wireless sensor networks," *International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC),* vol. 1, no. 2, 9-20, 2010. **DOI:** 10.5121/ijasuc.2010.1202

[23] L. Rajakumaran and R. Thamarai Selvi, "Detection techniques of sinkhole attack in WSNs: A survey," *International Journal of Engineering Science Invention,* vol. 3, no. 6, pp. 12-14, 2014.

[24] L. Teng and Y. Zhang, "SeRA: A secure routing algorithm against sinkhole attacks for mobile wireless sensor networks," in *IEEE Conference on Computer Modeling and Simulation,* 2010. **DOI:** 10.1109/iccms.2010.95

[25] Pooja, M and Singh, Y, "Security issues and sybil attack in wireless sensor networks," *International Journal of P2P Network Trends and Technology*, vol. 1, no. 3, pp. 7-13, 2013.

[26] S. Mohammadi, R. A. Ebrahimi and H. Jadidoleslamy, "A comparison of routing attacks on wireless sensor networks," *International Journal of Information Assurance and Security (JIAS),* vol. 6, pp. 195-215, 2011.

[27] N. Sultana and M. A. Islam, "Ubiquitous future M-Health system including wireless 3G technologies in Bangladesh," *Journal of Advances in Technology and Engineering Research,* vol. 1, no. 1, pp. 22-29, 2015. **DOI:** 10.20474/jater-1.1.3

— This article does not have any appendix. —

ISSN: 2414-4592
DOI: 10.20474/jater-3.1.5