International Journal For Technological Research In Engineering
Volume 4, Issue 10, June-2017 *ISSN (Online): 2347 - 4718*

SINKHOLE ATTACK IN WIRELESS SENSOR NETWORK

Neha Thakur[1], Asst Prof. Mrs Prachi Shahare[2]
M.Tech-CSE IV Semester (Multimedia Technology),
Department of Computer Science & Engineering, Kalinga University, Naya Raipur (C.G)

ABSTRACT: In a wireless sensor network, multiple nodes would send sensor readings to a base station for further processing. It is well-known that such a many-to-one communication is highly vulnerable to the sinkhole attack, where an intruder attracts surrounding nodes with unfaithful routing information, and then performs selective forwarding or alters the data passing through it. A sinkhole attack forms a serious threat to sensor networks, particularly considering that such networks are often deployed in open areas and of weak computation and battery power. In this paper, we present a novel algorithm for detecting the intruder in a sinkhole attack. The algorithm first finds a list of suspected nodes, and then effectively identifies the intruder in thelist through a network flow graph. The algorithm is also robust to deal with cooperative malicious nodes that attempt to hide the real intruder. We have evaluated the performance of the proposed algorithm through both numerical analysis and simulations, which confirmed the effectiveness and accuracy of the algorithm. Our results also suggest that its communication and computation overheads are reasonably low for wireless sensor networks.

I. INTRODUCTION

Wireless sensor networks become increasingly popular to solve such challenging real-world problems as industrial sensing and environmental monitoring. A sensor network generally consists of a set of sensor nodes, which continuously monitor their surroundings and forward the sensing data to a sink node, or base station. It is well-known that such a many-to-one communication is highly vulnerable to the sinkhole attack, where an intruder attracts surrounding nodes with unfaithful routing information, and then alters the data passing through it or performs selective forwarding. A sinkhole attack prevents the base station from obtaining complete and correct sensing data, and thus forms a serious threat to higher-layer applications. It is particularly severe for wireless sensor networks given the vulnerability of wireless links, and that the sensors are often deployed in open areas and of weak computation and battery power. Although some secure or geographic based routing protocols resist to the sinkhole attacks in certain level sensor networks are susceptible to the sinkhole attack In this paper, we propose a novel light-weighted algorithm for detecting sinkhole attacks and identifying the intruder in an attack. We focus on a general many-to-one communication model, where the routes are established based on the reception of route advertisements. Our solution explores the asymmetric property between the sensor nodes and the base station, and makes effective use of the relatively-high computation and communication power in the base station [2, 3, 4]. It consists of two steps: First, a secure and low-overhead algorithm for the base station to collect the network flow information with a distributed fashion in the attack area; and second, an efficient identification algorithm that analyzes the collected network flow information and locate the intruder. We also consider the scenario that a set of colluding nodes cheat the base station about the location of the intruder. Specifically, we examine multiple suspicious nodes and conclude the intruder based on majority votes. We show that such a conclusion is correct if less than half of the collected information comes from malicious nodes. The performance of the proposed algorithm is evaluated through both numerical analysis and simulations, which confirmed the effectiveness and accuracy of the algorithm. Our results also suggest that its communication and computation overheads are reasonably low for wireless sensor networks.

II. SINKHOLE ATTACK

Sinkhole attack is an insider attack were an intruder compromise a node inside the network and launches an attack. Then the compromise node try to attract all the traffic from neighbour nodes based on the routing metric that used in routing protocol. When it managed to achieve that, it will launch an attack. Due to communication pattern of wireless sensor network of many to one communication where each node send data to base station, makes this WSN vulnerable to sinkhole attack. The following subsections discuss the techniques use in MintRoute protocol and AODV protocol in launching sinkhole attack

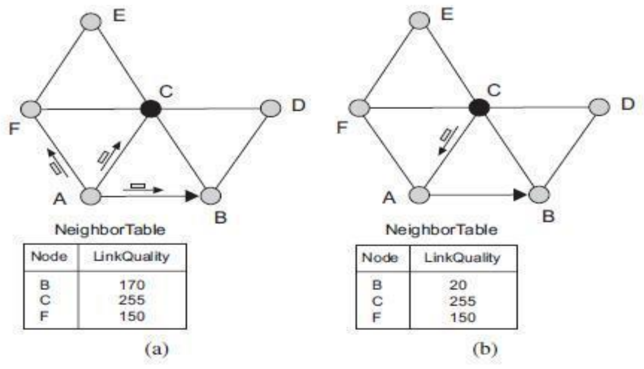

Figure 1: Sinkhole attack in MintRoute protocol

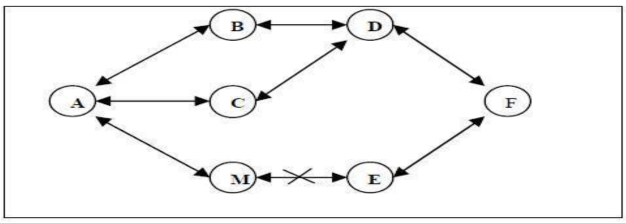

Figure 2: Sinkhole in Tiny AODV protocol

Sinkhole Attack in MintRoute Protocol

MintRoute protocol is a type of protocol which is commonly used in wireless sensor network. It was designed purposely for the wireless sensor network, it is light and suitable for sensor nodes which have minimum storage capacity, low computation power and limited power supply. MintRoute protocol uses link quality as a metric to choose the best route to send packet to the Base Station.

Figure.1 Shows six sensor nodes A, B, C, D, E, and F. Node C is malicious, and it is going to launch a sinkhole attack. The Figure 1(a) shows a route table of node A with IDs of its neighbors with their corresponding link quality. Originally the parent node was node B but node C advertises its link quality with a value of 255 which is maximum value. Node A is not going to change its parent node until the node B's link quality fall to 25 below the absolute value. In Figure.1(b) the malicious node is sending new update route packet that the link quality fall up to 20 and impersonate node B so that node A believe the packet come from node B. Node A will update its route table and change the parent node to node C The attacker uses node impersonation to launch an attack.

Sinkhole Attack in TinyAODV Protocol

This is another explanation of sinkhole attack in wireless sensor network and this time the attack is launched under TinyAODV (Ad-hoc On Demand Vector) protocol. TinyAODV protocol is the same as AODV in MANET but this one is lighter compared to AODV and it was modified purposely for wireless sensor network [27]. The number of hops to base station is the routing metric that used in this protocol. Generally the route from source to destination is created when one of the nodes send a request, the source node sends a RREQ (Route request) packet to his neighbors when wants to send packet. Next one of the neighbors close to destination is reply by sending back RREP (Route Reply) packet, if not the packet is forwarded to other nodes close to that destination. Finally, the source receives RREP packet from neighbor then select one node with less number of hops to destination.

The sinkhole node or compromised node launches an attack by send back RREP packet. In RREP packet it gives small number of hops which indicates close proximity to the base station. Then the source node decides to forward packet to sinkhole node. The compromised node then performs the same technique to its entire neighbors and tries to attract as much traffic as possible.

For instance, Fig.2 shows node M launches sinkhole attack in Tiny AODV. Node A sends RREQ to nodes BCM. However node M instead of broadcast to node E like nodes B and C does to node D, he replies back RREP to node A. Then node A will reject node B and C, then forward packet to M because node A and B are very far to F compare to node M.

III. CHALLENGES IN DETECTION OF SINKHOLE ATTACK IN WSNs

Based on the literature review of sinkhole attack in wireless sensor network, the following are the main challenges in detecting sinkhole attack in wireless sensor network

A. Communication Pattern in WSN;

All the messages from sensor nodes in wireless sensor network are destined to base station. This created opportunity for sinkhole to launch an attack. Sinkhole attacks normally occur when compromised node send fake routing information to other nodes in the network with aim of attracting as many traffic as possible. Based on that communication pattern the intruder will only compromised the nodes which are close to base station instead of targeting all nodes in the network. This is considered as challenges because the communication pattern itself provides opportunity for attack.

B. Sinkhole attack is unpredictable;

In wireless sensor network the packet are transmitted based on routing metric that used by different routing protocols [26]. The compromised node used its routing metric that used by routing protocol to lie to his neighbors in order to launch sinkhole attack. Then all the data from his neighbors to base station will pass through compromised node. For example the techniques used by compromised node in network that used TinyAODV protocol is different to the one used another protocol like MintRoute protocol. In MintRoute they used link quality as route metric while in Tiny AODV they used number of hop to base station as routing metric. Therefore the sinkhole attack techniques is changed based on routing metric of routing protocol

C. Insider Attack;

Insider attack and outsider attack are two categories of attack in wireless sensor network. Outside attack is when intruder is not part of network. In inside attack the intruder compromises one of the legitimate node through node tempering or through weakness in its system software then compromised node inject false information in network after listen to secret information. Inside attack can disrupt the network by modifying routing packet. Through compromised node sinkhole attack attract nearly all the traffic from particular area after making that compromised node attractive to other nodes. The fact is that compromised node possesses adequate access privilege in the network and has knowledge pertaining to valuable information about the network topology this created challenges in detecting. Base to that situation even cryptographic cannot defend against insider attack although it provides integrity, confidentiality and authentication (Pathan, K [22]). Therefore the internal attack has more serious impact on victim system compared to outsider attack.

D. Resource Constraints;

The limited power supply, low communication range, low memory capacity and low computational power are the main constrained in wireless sensor network that hinder implementation of strong security mechanism. For example the strong cryptographic method that used in other network cannot be implemented in this network due to low computational power and low memory capacity. Therefore less strong key are considered which is compatible with available resources.

E. Physical attack;

A wireless sensor network normally deployed in hostile environment and left unattended. This provides a opportunity for an intruder to attack a node physically and get access to all necessary information

IV. WIRELESS SENSOR NETWORK SECURITY ISSUES

In this section of the paper we discuss various issues concern with the security of WSNs including limitations, unreliability, etc.

A. Sensor networks: The limitations

A distributed sensor network (usually heterogeneous) consists of hundreds to thousands of low-cost and low-power small sensors that are interconnected through a communication network. The sensors are embedded devices that are networked via wireless media, usually integrated with a physical environment, and are capable of acquiring and processing the signals along with communicating and performing simple computational tasks. Common functions of WSNs are broadcasting, multicasting, routing, forwarding, and route maintenance. The vast applications of sensor networks highlight a vision in which a large number of tiny sensor nodes will be embedded in almost every aspect of human everyday life. However, the widespread deployment of sensor nodes and their overall success is directly related to their security strength. Though WSNs are capable of collecting large amount of information, recognizing significant events and responding appropriately, the need for security is obvious in WSNs. WSNs have many constraints from which results in new challenges. The sensor nodes have extreme resource limitations and unreliable communication medium and that too in unattended environments which make it very difficult for the employment of the existing security approaches due to the complexity of the algorithms working for sensor platform. The understanding of these challenges inside WSNs provides a basis for further works on sensor networks security. The extreme resource limitations of sensor nodes pose considerable challenges due to resource-hungry security mechanisms. In order to effectively implement approaches, required amount of data memory, code space, and energy is required. However, due to small size of sensor nodes, these resources are very limited [1].

1) Limited memory and storage

The memory of tiny sensor nodes usually ranges from 2 KB to 256 KB while the storage ranges from 32 KB to 2 GB. Table 1 provides the commonly available sensor nodes with memory and storage. Such hardware constraints of sensor nodes necessitate extremely efficient security algorithms in terms of computational complexity, bandwidth, and memory. The limitation of memory and storage makes it very difficult to implement highly efficient security mechanisms requiring more memory.

2) Limited power

Energy (power) is the biggest constraint in wireless sensor capabilities. It is one of the main reason that nodes are subject to failures because of depletion of batteries, or more general, it is due to environmental changes. Sensor nodes need to operate autonomously for prolonged periods of time after deployment and it is not possible to easily replace or recharge the batteries. Therefore, the energy consumption must be minimized for long life; this necessitates both the power efficiency of the hardware along with the efficiency of security and other protocols.

Table 1: Selection of commonly available sensor nodes

Platform	MCU	RAM	Program & Data Memory	Radio Chip
BTnode3	ATMega128	64 KB	128 - 180 KB	CC1000/Bluth
Cricket	ATMega128	4 KB	128 - 512 KB	CC1000
Imote2	Intel PXA271	256 KB	32 - MB	CC2420
MICA2	ATMega128	4 KB	128 - 512 KB	CC1000
MICAZ	ATMega128	4 KB	128 - 512 KB	CC2420
Shimmer	TI MSP 430	10 KB	48 KB - Up to 2 GB	CC2420/Bluth
TelosA	TI MSP 430	2 KB	60 -512 KB	CC2420
TelosB	TI MSP 430	10 KB	48 KB - 1 MB	CC2420
XYZ	ARM 7	32 KB	256 - 256 KB	CC2420

B. Unreliability of communication

One of the major threats to sensor security is the very nature of the wireless communication medium, which is inherently insecure. The wireless medium is open and accessible to anyone unlike wired networks, where a device has to be physically connected to the medium. Due to this any transmission can easily be intercepted, altered, or replayed by an adversary. Intruder can easily intercept valid packets and inject malicious ones due to open access nature of wireless communication medium. Furthermore, damaging of packets may take place due to unreliable transmission channels, this may be result of channel errors or high congestion in sensor nodes. Even communication may still be unreliable in the case of reliable channels also. Conflicts may occur due to packets colliding meet in the middle of transfer resulting in failure of transfer. Such weakness can be easily exploited by an intruder having a strong transmitter, and can easily produce interference (like jamming)

C. Deployment and immense scale

A high degree of dynamics in WSNs is caused due to node mobility, node failures, and environmental obstructions. Frequent topology changes and network partitions are the reasons for this. Sensor node can be deployed in large areas which is one of the most attractive characteristics of WSNs ability. Thousands or millions of nodes, without any prior knowledge on their position can be deployed making the structure of the network complicated. It is therefore required that efficient security schemes can operate within this dynamic environment. It is a substantial task of networking tens to hundreds or thousands of nodes and implementing security over such a network is equally challenging too. More robust security techniques are needed to cope with such dynamics of ever-changing nature of sensor networks. At the same time changes in the network membership needs to be supported in an equally efficient and secure manner. There should be transparency regarding node device joining/leaving the network and a minimum amount of information should have to be reconfigured.

D. Operation unattended

The hostile environment in another challenging factor in which sensor nodes function. Nodes may be left unattended for long periods of time depending on the application which exposes them to physical attacks. Sensor nodes face the possibility of destruction or capture and compromise by attackers. Nodes are compromised when an attacker gains control of a node after deployment in the network. A compromised node may be physically damaged or forced to non-functional, even sensor nodescharacteristics/mechanisms may be altered to send out data readings of intruders choice. After gaining control, the attacker can alter the node in order to listen to information in the network and input malicious data or perform a variety of attacks. Intruder may also disassemble the node in order to extract information vital to the network's security including routing tables, data, and cryptographic keys. The absence of any fixed infrastructure enhances this vulnerability due to lack of central controller to monitor the operation of the network and in order to identify intrusion attempts. Most of such networks have a designated base station but, its role is typically limited to data collection and query distribution, and it does not include any form of actual control. As a result of this, security mechanism has to be implemented as a cooperative and distributed effort of all the network nodes. This issue is further complicated by the difficulty in differentiating between trustworthy nodes from compromised ones. A compromised node still is capable of generating valid network data along with distributing it around in order to appear functionally stable. This is going to prevent cooperating nodes from taking measures against their corrupt neighbours who continue to rely on the fake information being fed to them.

V. WSNs SECURITY REQUIREMENTS

In this section of the paper we discuss requirements that are concern with the security of WSN. Sensor networks are a type of distributed networks and share some commonalities with a typical computer network, at the same time pose unique requirements and constraints. Therefore, security goals for WSN encompass both the typical network requirements and the special unique requirements suited for WSNs. The security requirement of WSN must include attributes such as confidentiality, integrity, data freshness, availability, and authentication. All network models allow provisions for implementing above said properties in order to assure protection against attacks to which these types of networks are vulnerable. In the following, standard security requirements (and eventually behavior) for the sensor network are discussed.

A. Confidentiality of data

Data confidentiality is the ability to conceal network traffic from an attacker so that any communication via the sensor network remains secret and is the most important issue concern with network security. In many applications (like key distribution) nodes communicate secret and highly sensitive data. The approach commonly used for keeping sensitive data secret is to encrypt it with a secret key that only intended receivers possess, therefore achieving confidentiality. Public-key cryptography is very expensive to be used in the resource constrained sensor networks and therefore most of the proposed protocols make use of symmetric key encryption methods. Furthermore, confidentiality only guarantees the security of communications inside the sensor network, it does not prevent the misuse of information that reaches the base station. It is therefore required that information must be coupled with the right control policies so that unauthorized users can be prevented from having access to confidential information.

B. Authentication & integrity of data

False messages can be easily inject in a sensor network by an attacker, therefore the receiver needs to insure that the data to be used in any decision- making process is valid. Data integrity and authentication is therefore necessary to enable sensor nodes for detecting modified, injected, or replayed packets. Not only authentication of safety-critical applications is required, it is still needed for rest of applications otherwise the user of the sensor network may get the wrong information of the sensed world thus making decisions inappropriate. Symmetric or asymmetric mechanisms are used for achieving data authentication is in case sending and receiving nodes share secret keys. It is extremely challenging to ensure authentication due to the wireless and unattended nature of sensor networks that may cause data loss or damage. Authentication alone does not resolve the problem of node takeovers since compromised nodes can be still authenticated by themselves in the network. Therefore authentication mechanisms should be collectively used for aiming at securing the entire network. Intrusion detection techniques may be used to locate the compromised nodes for starting appropriate revoking procedures.

C. Availability of data

Availability is concern with the ability of a sensor node to use the resources and whether the sensor network is available for the communication of messages. A sensor network has to be robust against various security attacks, and impact should be minimized of a succeeded attack. However, it is extremely difficult to ensuring network availability due to limited ability of individual sensor nodes to detect between threats and failures.

D. Freshness of data

Data freshness implies that the available data is recent, and it also ensures that any old messages are not replayed by adversary. Freshness of data can be provided by inserting sequence numbers into the packets for sorting the old ones out. All the above discussion suggests that it is very necessary to develop sensor networks that exhibit autonomic security capabilities, i.e., the networks are resilient to attacks and they have the ability to recover damage after an intrusion. Security architecture for WSNs must integrate a sufficient number of security measures and techniques for protecting the network and to satisfy the desirable requirements as outlined.

VI. ATTACKS IN WSN

As mentioned earlier, due to the unique characteristics of underlying networking protocols, sensor networks are vulnerable to security threats. Attacks can occur at any layer such as physical, link, network, transport, and application etc. Most of these routing protocols are not designed to have security mechanisms and it makes it even easier for an attacker to break the security for example, attacks at the physical layer of the network include jamming of radio signal, tampering with physical devices etc. In the following section we discuss in detail the layer wise attacks in WSNs

A. Physical layer attacks

Jamming – It is caused due to interference with the radio frequencies of the network's devices which is an attack on the availability of the sensor network. It is different from normal radio propagation in the way that it is unwanted and disruptive, thus resulting in denial-of-service conditions.

Tampering – It is also called node capturing in which a node is compromised, it is easy to perform and is pretty harmful. Tampering is physically modifying and destroying sensors nodes.

B. Link layer attacks

Collision – It is caused in link layer that handles neighbor-to-neighbor communication along with channel arbitration. Entire packet can be disrupted if an adversary is able to generate collisions of even part of a transmission, CRC mismatch and possibly require retransmission can be caused by a single bit error.

Exhaustion – Exhaustion of a network's battery power can be induced by an interrogation attack. A compromised node could repeatedly send thus consuming the battery power more than required.

Table 1: Attacks on different layers in WSN

Layer	Attack
Physical	Jamming, Tampering
Link	Collision, Exhausting
Network	Hello flood, Wormhole, Sybil, Sinkhole
Transport	Flooding
Application	Denial-of-Service, Cloning

C. Network layer attacks

Hello flood attack – It is caused when an attacker with high transmission power can send or replay hello packets which are used for neighbour discovery. In this way, attacker creates an illusion of being a neighbor to other nodes and underlying routing protocol can be disrupted which facilitate further types of attacks.

Wormhole attack – It is caused due to formation of a low-latency link that is formed so that packets can travel from one to the other end faster than normally via a multi-hop route. The wormhole attack is a threat against the routing protocol and is challenging to detect and prevent. In this type of attack, an adversary can convince the distant nodes that are only one or two hops away through the wormhole causing confusion in the network routing mechanisms.

Sybil attack – It is caused when an attacker uses a malicious device to create a large number of entities in order to gain influence in the network traffic. The ID of these malicious nodes can be the result due to fake network additions or duplication of existing legitimate identities. The sybil attack usually targets fault tolerant schemes including distributed storage, topology maintenance, and multi-hop routing.

Sinkhole attack – It is caused when an attacker prevents the base station of the network from obtaining complete and accurate sensing data, thus resulting in a serious threat to higher-layer applications. By Sinkhole attack, attacker can attract nearly all the traffic from a specific area. Sinkhole attacks work in the way by making malicious node look especially attractive to other surrounding nodes with respect to routing protocols underling routing algorithm.

D. Transport layer attacks

Flooding attack – It is a Denial of Service (DoS) attack designed to bring a network or service down by flooding it with large amounts of traffic. Flood attacks usually occur when a network or service becomes weighed down with packets, thus initiating incomplete connection requests that it cannot, longer process genuine connection requests. By flooding a server with connections that cannot be completed, flood attack eventually fills the servers memory buffer and once this buffer is full, no further connections can be made, and thus resulting in a Denial of Service.

E. Application layer attacks

Denial-of-Service (DoS) – This attack is usually referred as intended attack of opponent for the purpose of destroying or destructing the sensor network. DoS attack may result in limiting or eliminating the sensor network functionality than expected. DoS attack may occur at any layer of OSI layers of WSN. DoS penetrates the efficiency of targeted networks by affecting its associated protocols by consuming the resources, destructing or altering the infrastructure configuration, and physically destroying the network components.

Cloning attack – It is caused when adversaries may easily capture and compromise sensors nodes and deploy unlimited number of clones in the sensor network of the compromised nodes. As these clones have legitimate access to the sensor network (i.e. legitimate IDs, keys, other security credentials, etc.), they can easily participate in the sensor network operations in the same way as a legitimate node resulting in a large variety of insider attacks, or even taking over the entire network. If these clones in the sensor network are left undetected, the sensor network is unshielded to attackers, thus extremely vulnerable. That is why clone attackers are severely destructive. Effective and efficient solutions are required for clone attack detection to limit their damage.

VII. CONCLUSION AND FUTURE WORK

Based on existing works most researchers are trying to look for ICT solutions for detecting, identifying and providing resistance to sinkhole attack in wireless sensor network. Researchers used intrusion detection scheme based on anomaly-method, other used rule based and key management to detect and identifying the sinkhole nodes. Majority of researches struggled with security challenges corresponding with availability of resources and mobility of wireless sensor nodes. Some provided solution for only static and few on mobile network. Very few researchers managed to validate their security system using real wireless sensor network. Also some of results showed low detection rate, high network overhead and high communication cost. The future solution should focus on reducing high network overhead, computational power, increase detection rate and that system must be validated in real sensor network. Through this kind of validation, it will be easy to check if their solutions meet the available resources of WSN, such as memory capacity.

REFERENCES

[1] Abhishek Pandey and R.C. Tripathi. (2010). A Survey on Wireless Sensor Networks Security, International Journal of Computer Applications (0975 – 8887) Volume 3 – No.2.

[2] Changlong Chen, Min Song, and George Hsieh (2010) Intrusion detection of Sinkhole attack in large scale Wireless Sensor Networks, In Wireless Communications, Networking and Information Security (WCNIS), 2010 IEEE International Conference on (pp.711-716).IEEE

[3] Chen, C., Song, M. and Hsieh, G. (2010). Intrusion Detection sinkhole attack in large scale wireless sensor network, In Wireless Communication, Networking and Information Security (WCNIS), 2010 IEEE Interational Conference on (pp. 711-716). IEEE.

[4] Choi, G. B., Cho, J. E., Kim,H. J., Hong, S. C. and Kim, H. J. (2008).A sinkhole attack detection mechanism for LQI based mesh routing in WSN. In ICOIN

[5] Jaydip Sen. (2009). A Survey on Wireless Sensor Network Security, International Journal of Communication Networks & Information Security, 1(2).

[6] Kalpana Sharma and M K Ghose. (2010) Wireless Sensor Networks: An Overview on its Security Threats, IJCA, Special Issue on “Mobile Ad-Hoc Networks” MANET.

[7] Krontiris,I., Dimitriou,T., Giannetsos,T. and Mpasoukos, M. (2008). Intrusion Detection Sinkhole Attacks in Wireless Sensor Network. In Networking and Communications, 2008. WIMOB’08. IEEE Interational Conference onWireless and Mobile Computing, (pp. 526-531). IEEE.

[8] Krontiris, I., Giannetsos, T. and Dimitriou, T. (2008). Launch Sinkhole Attack in Wireless Sensor Network; the Intruder Side. In Networking and Communications, 2008. WIMOB’08. IEEE International Conference on Wireless and Mobile Computing, (pp. 526-531). IEEE.

[9] Krontiris, I. Dimitrou, T. Freiling, F.C. (2007). Towards intrusion detection in wireless sensor networks. In Proc. Of the 13th European Wireless Conference.

[10] Liping Teng and Yongping Zhang. (2010). SeRA: A Secure Routing Algorithm against Sinkhole Attacks for Mobile Wireless Sensor Networks, In Computer Modelling and Simulation, 2010. ICCMS’10. Second International Conference on (Vol. 4, pp. 79-82).

[11] Chelli P, “ Security Issues in Wireless Sensor Networks: Attacks and Countermeasures,” Proceedings of the World Congress on Engineering 2015, Vol. 1, WCE 2015, July 13 3, 2015, London, U.K.

[12] Munish Dhar and Rajeshwar Singh, “A Review of Security Issues and Denial of Service Attacks in Wireless Sensor Networks,” International Journal of Computer Science and Information Technology Research, Vol. 3, Issue 1, March 2015, ISSN 2348-1196 (print), ISSN 2348-120X (online).

[13] Genita Gautam, Biswaraj Sen, “Survey on different types of Security Threats on Wireless Sensor Networks,” International Journal of Computer Science and Information Technologies, Vol. 6, 2015, ISSN: 0975-9646.

[14] Kanchan Kaushal and Taranvir Kaur, “A Survey on Attacks of WSN and their Security Mechanisms,”International Journal of Computer Applications, Volume 118, No. 18, May 2015.

[15] Sahabul Alam and Debashis De , “ Analysis of security threats in wireless sensor network,” International Journal of Wireless & Mobile Networks (IJWMN), Vol. 6, No. 2, April 2014.

[16] Hosam Soleman and Dr. Ali Payandeh , “ Self-protection mechanism for wireless sensor networks,” International Journal of Network Security & Its Applications (IJNSA), Vol. 6, No. 3, May 2014.

[17] Raja Waseem Anwar , Majid Bakhtiari, Anazida Zainal, Abdul Hanan Abdullah and Kashif Naseer Qureshi, “Security Issues and Attacks in Wireless Sensor Network,” World Applied Sciences Journal 30 (10): 1224-1227, 2014 ISSN 1818-4952.

[18] Naser Alajmi , “ Wireless Sensor Networks Attacks and Solutions,” (IJCSIS) International Journal of Computer Science and Information Security, Vol. 12, No. 7, July 2014.

