INTERNATIONAL JOURNAL OF ADVANCE RESEARCH AND DEVELOPMENT

(Volume2, Issue2)

Available online at: www.ijarnd.com

Survey on Mechanisms to detect and mitigate the impact of Sinkhole Attack in Wireless Sensor Networks

Amulya D, C N Chinnaswamy

Student, Associate Professor

Department of Information Science and Engineering the National Institute of Engineering Mysuru, India

eshu1412@gmail.com, chinnaswamynie@gmail.com

Abstract

Sinkhole attack is an active attack, launched in a Wireless Sensor Network by compromising a legitimate node or by introducing a malicious node in order to gain the traffic routed towards it before reaching the base station, by making a false advertisement in the routing information of its nearest distance to reach the base station. Due to this fake information the data packets under transmission are routed towards the malicious node through which the attacker can gain the access to the information, tamper the information or may even destroy it. Thus, this attack causes a severe threat to the normal functionality of the Wireless Sensor Network. Because of the wider range of applicability of Wireless Sensor Networks in our day-to-day life and in future the detection and mitigation of Sinkhole attack plays a vital role. In this view, a survey on the existing mechanisms to detect and mitigate the Sinkhole attack, their advantages and drawbacks is being documented by us in this paper.

Keywords-Wireless Sensor Networks (WSN), Sinkhole Attack, Intrusion Detection System (IDS), base station.

I. INTRODUCTION

Wireless sensor networks (WSNs) have drawn fair amount of research attention during last decade. Their limited resources along with the hostile deployment environment put severe challenges to the research studies. Various aspects of such networks have been already studied and these types of networks are now well established for many applications ranging from habitat monitoring to surveillance [24].Security is a vital concern in WSNs. Without availability, data confidentiality and integrity many real-world applications of WSNs are in vain. As a result, many studies have been focused on providing security solutions for these networks [25]. Detection and mitigation of attacks against WSNs has been an attractive topic amongst researchers, especially, considering the unique challenges of these networks which are mainly imposed by their resource constraints. Many types of attacks have been introduced, analyzed and eliminated in the literature [25, 26]. Sinkhole attack is one of the earliest among them that has been identified in WSNs [27]. Sinkhole attack threatens the security of WSNs at almost every layer of their protocol stack. The main deception of the attack is that a malicious node attracts the traffic of its neighbors by pretending that it has the shortest path to the base station. The attack may jeopardize many important security measures. The sinkhole may launch a variety of attacks against the data traffic, such as selectively dropping the data packets, tampering data aggregation algorithms or interfering with clustering protocols. Various approaches have been proposed to combat the attack either by manipulation of routing algorithms [28, 29] or by utilization of IDS [4, 30].

Sinkhole attack is an active and intruder attack where an attacker or intruder launches the attack either by introducing a malicious node or by compromising an existing node in the network to act as malicious node. The malicious node attracts the network traffic from all its neighbor nodes towards it by advertising a false optimal

path information regarding the reachability to the base station through the malicious node and this routing information used by the routing metric in order to choose the best path by the implemented routing protocols leads to the launch of the sinkhole attack successfully in the network. Thus, the malicious node successfully avoids the base station from receiving the complete and the correct messages from the other nodes in the network. The many to one communication pattern where each individual node sends data to the base station makes the WSN vulnerable to the sinkhole attack. Sinkhole attack can be launched by introducing a malicious node that does not necessarily target all the nodes in the network but intendedly targets those nodes which are close to the base station. Sinkhole attack in a network is demonstrated with a simple example as shown below. The network structure in Figure 1 shows the organization of nodes without any sinkhole attack. In this structure, node 3 communicates with the base station via node 2 since node 2 has the shortest reachability to base station than node 1. Similarly, the structure in Figure 2 shows the network organization with node 1 being the malicious node for the sinkhole attack. In this scenario node 3 communicates with the base station via node 1 because of the false advertisement of the shortest reachability made by node 1.

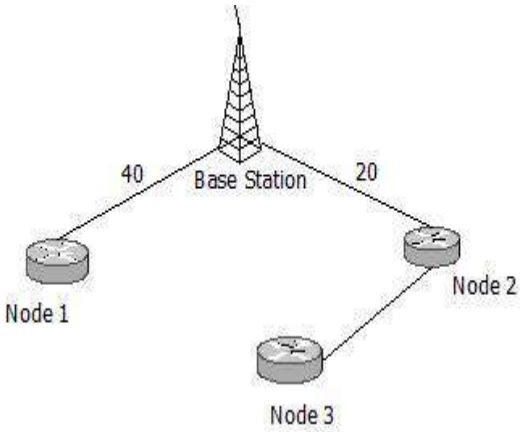


Figure 1. WSN without Sinkhole attack

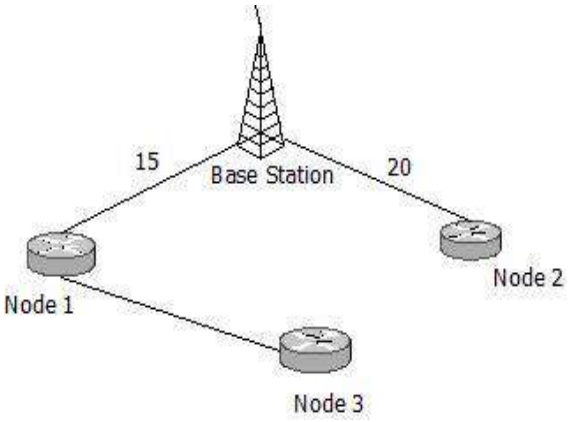


Figure 2. WSN with Sinkhole attack

II. CHALLENGES IN DETECTING THE SINKHOLE ATTACK

The review through literature surveys on sinkhole attack has provided the basis to identify the challenges in the detection of sinkhole attacks in the wireless sensor networks. The main challenges are as follows,

A. Communication Patterns in WSN

The many to one communication pattern of the wireless sensor network provides the opportunity for the sinkhole attack because the messages delivered to the base station from all the sensor nodes are directed via other nodes in the routing path selected by the routing metrics. Thus, the intruder can launch the attack based on the communication pattern by compromising the nodes that are close to the base station. Hence the design and maintenance of the communication pattern poses a challenge for detecting the sinkhole attack.

B. Dynamic Nature of WSN

The mobility of the sensor nodes in the WSN with the routing pattern built as sensors and base station makes the location identification of the sensor node a different task. This provides an opportunity for the intruder to launch the attack by introducing a malicious node randomly at some region near to the base station. Thus, the detailed tracking and maintenance of dynamicity information of the nodes is a challenge to detect the attack.

C. Unpredictable Nature of Sinkhole Attack

The communication in the WSN happens through the packet transmission via the path selected by the routing metrics used by the routing protocols. Thus, the attack will be launched by the compromised node which is specific to the routing metric used by the protocol of the network under threat. Hence, the sinkhole attack remains unpredictable to be detected with common mechanism in all the networks.

D. Insider Attack

Sinkhole attack can be launched as an Insider attack. In this technique, the attacker or the intruder comprises one of the legitimate nodes of the network to become the malicious node by node tampering or through the weakness in the system software of the node. Once the node is compromised the attacker disrupts the network by modifying the routing packets. The compromised node contains sufficient knowledge pertaining to the topology of the network and will also have adequate access privileges in the network. Hence this situation creates additional challenges in the detection of sinkhole attack.

E. Resource Constraints limit Detection Methods

The resource constraints such as limited power supply, lower communication range, low capacity for memory and limited computational ability of the sensor nodes hinder the implementation of stronger security mechanisms. Low computational power and limited memory capacity makes the implementation of strong cryptographic methods infeasible in WSN. Thus, the adaptations of weaker security mechanisms that are compatible with the available resources provide an opportunity to launch attack.

F. Physical Attack Vulnerability

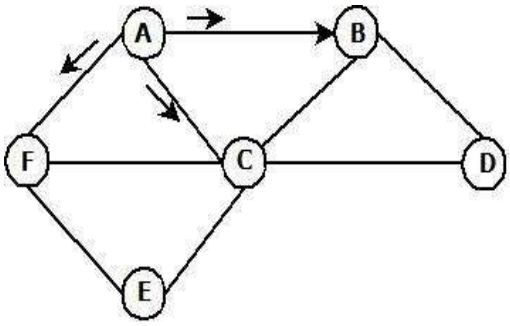
The deployment of WSN in a hostile environment and being unattended provides an opportunity for the intruder to attack the node physically and gains the necessary information with respect to the network structure and communication pattern.

III. TECHNIQUES USED IN LAUNCHING SINKHOLE ATTACK

The following subsections discuss the techniques used in Mint Route protocol and AODV protocol in launching sinkhole attack.

A. Sinkhole Attack in MintRoute Protocol

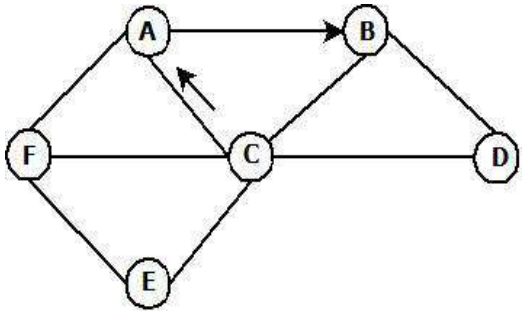
Mint Route protocol is a type of protocol which is commonly used in wireless sensor network. It was designed purposely for the wireless sensor network; it is light and suitable for sensor nodes which have minimum storage capacity, low computation power and limited power supply. Mint Route protocol uses link quality as a metric to choose the best route to send packet to the Base Station (Krontiris et al [4]). Figure 3 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 3(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.



Neighbor Table

Node	Link Quality
B	170
C	255
F	150

(a)



Neighbor Table

Node	Link Quality
B	20
C	255
F	150

(b)

Figure 3. Sinkhole Attack in MintRoute Protocol

In Figure 3(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 (Krontiris et al [4]). The attacker uses node impersonation to launch an attack.

B. Sinkhole Attack in TinyAODV Protocol

This is another technique of launching the sinkhole attack in wireless sensor network and this time the attack is launched under Tiny AODV (Ad-hoc On Demand Vector) protocol. Tiny AODV 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 [23]. 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.

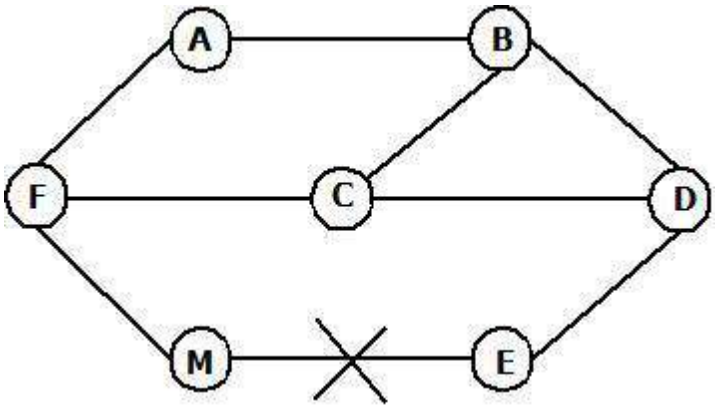


Figure 4. Sinkhole Attack in Tiny AODV Protocol

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 [23].

For instance, Figure 4 shows node M launches sinkhole attack in Tiny AODV. Node F sends RREQ to nodes A, C, M. However node M instead of broadcast to node E like nodes A and C does to node D, he replies back RREP to node F. Then node F will reject node A and C, then forward packet to M because node F and A are very far to D compare to node M.

IV. APPROACHES TO PREVENT AND DETECT SINKHOLE ATTACK

Due to wide popularity and adaptability of the wireless sensor networks the requirement to provide security mechanisms that suits the resource constraint challenge has given a wide platform for the researchers. Based on such research works, different approaches to detect and prevent the sinkhole attacks have been identified and listed. The approaches are classified as rule based, anomaly based, statistical method, hybrid based and prevention based. The classification is shown in Figure 5.

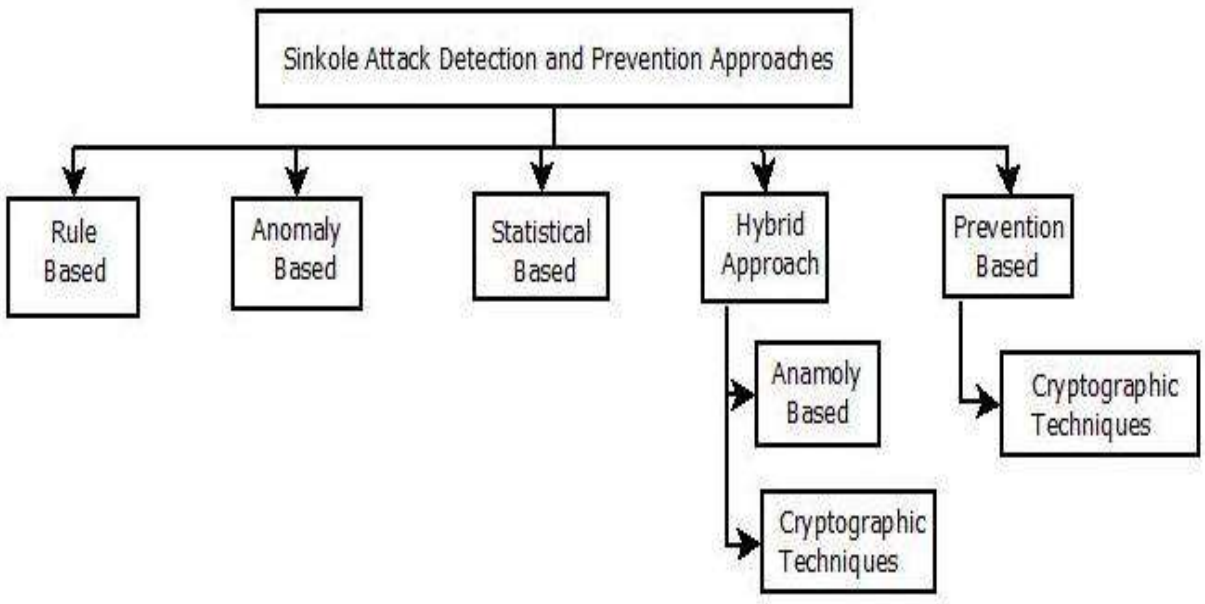


Figure 5. Classification of approaches to prevent and detect Sinkhole Attack

The following subsections give a brief description of these approaches.

A. Rule Based

This approach deals with the designing and defining the rules based on the technique and behaviors used by the attackers to launch the sinkhole attack. The defined rules are implemented in the intrusion detection system that is adapted and being executed by each sensor node in the WSN. The packets under transmission in the network are analyzed with respect to the defined rules. The node which violates these defined rules is considered to be adversary and compromised and hence it will be isolated from the network.

B. Anomaly Based

It is a detection based approach where a differentiation between the normal user behavior and an anomalous activity in the network is defined and implemented in the intrusion detection system. Hence the detection of the attack in the network is achieved by considering intrusion as an anomalous activity since it will be abnormal with respect to the normal behavior of the legitimate user. Rule based and statistical methods form a subset under this category of detection approach.

C. Statistical Based

The analysis of the data associated with the nodes in the network with respect to certain activities is performed and recorded. This information is used by the statistical method to detect the attack in the network. For example, the monitoring of the normal packets in the network and their transmission patterns between the nodes is analyzed. The detection of the adversary is done by comparing the threshold value used as a reference with the actual behavior of the node, the node is considered as an intruder if its value exceeds than the threshold value.

D. Hybrid Based

Anomaly based and Cryptographic approaches are implemented in combination with each other in order to detect and prevent the sinkhole attack in the network, respectively. The combination of these two approaches forms the Hybrid approach. The usage of hybrid approach reduces the false positive rate that is produced by the anomaly based approach individually. The detection of malicious node can be achieved by defining the signature of the legitimate nodes in the database and the one whose signature being not defined is caught as being an intruder; this provides an advantage to the system.

E. Prevention Based

The cryptographic techniques such as the encryption and decryption keys are used to maintain the integrity and authenticity of the packets under transmission in the network. The packet is transmit is encrypted with the help of encryption key such that the access to the message can be obtained only with the availability of the decryption key and also helps in the identification of any small changes in the data during transmission. The authenticity mechanism provides the verification about the origin of the message from the base station and the legitimate nodes in the network.

V. MECHANISMS TO OVERCOME SINKHOLE ATTACK

A. Location-Based Compromise-Tolerant Security Mechanism

Many WSNs have an intrinsic property that sensor nodes are stationary, i.e., fixed at where they were deployed. This property has played an important role in many WSN applications such as target tracking [12] and geographic routing [13]. By contrast, its great potential in securing WSNs has so far drawn little attention. Based on this observation, Zhang proposed a suite of location-based compromise-tolerant security mechanisms for WSNs. To mitigate the impact of compromised nodes in WSN's, a Location-Based Compromise-Tolerant Security Mechanism [11] implements the notion of location-based keys (LBKs),based on a new cryptographic concept called pairing, for binding private keys of individual nodes to both their IDs and geographic locations. LBK-based neighborhood authentication scheme is then developed to localize the impact of compromised nodes to their vicinity. It introduces an efficient approach to establish pair wise shared keys between any two nodes that are either immediate neighbors or multi hop away. Such keys are fundamental in providing security support for WSNs. This approach features low communication and computation overhead, low memory requirements, and good network scalability.

LBKs can act as efficient countermeasures against some notorious attacks against WSNs. These include the Sybil attack [14], [15], the identity replication attack [15], wormhole and sinkhole attacks [14], and so on. Finally a location-based threshold-endorsement scheme, called LTE, is used to thwart the infamous bogus data injection attack, in which adversaries inject lots of bogus data into the network. Conclusively, there are enormous potential applications of LBKs in WSNs, such as misbehavior detection, secure distributed storage, secure routing, and target tracking.

B. Hop-Count Monitoring Scheme

To detect sinkhole attacks, we require an intrusion detection system (IDS) that recognizes abnormal route updates. Route advertisements from an attacker syntactically appear as legitimate advertisements, hence we cannot use a misuse [16] or signature based detection system. To address this problem, an anomaly detection scheme is used to detect abnormal route advertisements that are caused by sinkhole attacks.

This approach to detecting abnormal route advertisements is to monitor the advertised hop-count values. A significant change in the hop-count value is an indication of the presence of a sinkhole attack. A key research challenge in this approach is how to detect abnormal hop count values in a computationally efficient way within the resource constraints of wireless sensor nodes. In this schema, Daniel Dallas proposed an Anomaly Detection System (ADS) [17] in which the sinkhole detector was designed so as to discover an observable feature that reacts to the attack in a consistent manner so that it can be used to reliably trigger an alert. To create a sinkhole, the attacker needs to understate its distance, which is accomplished in distance vector routing protocols by claiming a low hop-count – representing a short distance. With hop-count forgery playing an intrinsic role in the success of a sinkhole attack, it was analyzed whether forged hop-counts would be conspicuous enough to reliably indicate the presence of an attack. It was found that physically static nodes have indicated that a reduction in hop-count will not occur except as a result of forging the hop-count value. Also evident was that when efficient routes are created from base station advertisements, large increases in hop-count are unlikely to occur simply due to traversing a slightly different set of nodes. Abnormally large increases in hop-count resulted from an abnormal route detour, which was likely to have occurred due to a failure in the more efficient path.

Therefore this schema watches for attacks when the hop count shifts abnormally low and watches for failures when the hop-count shifts abnormally high. Consequently, all variations in hop-count for anomalies were scrutinized, and the resulting IDS imposes thresholds on hop-count variation (representing variation in distance) when routing paths are updated. Hop-counts below the lower threshold become suspect attacks and hop-counts above the upper threshold indicate the failure of multiple nodes. Another challenge in the design of this intrusion detection scheme is where to locate the ADS in the network. Given the resource constraints of wireless nodes, it is important to avoid deploying the ADS on all nodes in the network. An alternative solution would be to deploy the ADS at the base station, and monitor the consistency of traffic arriving at the base station. However, a sinkhole attack can effectively disguise its presence – preventing detection from an ADS located at the base station – by restricting its broadcast so that the ADS does not hear the attack. The sinkhole can then forward all traffic through a wormhole to the base station. Consequently, these IDS can be deployed at multiple strategic locations in the sensor network in a decentralized manner. Since the hop-count feature is easily obtained from routing tables, the ADS system is simple to implement with a small footprint. Using single ADS, a detection rate of 96% was achieved with no false alarms for attacks in a simulated network [16]. In addition, by using a small number of ADSs at strategic locations in the network, a 100% detection rate was achieved [17].

C. Non Cryptographic method of Sinkhole Attack Detection

Recently, Mobile Agents have been proposed for efficient data dissemination in WSNs [18]. In a typical client/server based WSN, the occurrence of certain events will alert sensors to collect data and send them to a sink node. However, the use of Mobile Agents leads to a new computing paradigm, which is in marked contrast to the traditional client/server-based computing. The Mobile Agent is a special kind of software that propagates over the network either periodically or on demand (when required by the applications). It performs data processing autonomously while migrating from node to node. Q. Wu [19] presents a genetic algorithm based solution to compute an approximation to the optimal source-visiting sequence. The use of Mobile Agents in computer networks has certain advantages and disadvantages [20], such as code caching, safety and security, depending on the particular scenario. Regardless, they have been successful deployed in many applications ranging from ecommerce to military situation awareness [21]. As described in [18], many inherent advantages (e.g., scalability, extensibility, energy awareness, and reliability) of the Mobile Agent architecture make it more suitable for WSNs than the client/server architecture. In [22], Mobile Agents are found to be particularly useful for data fusion tasks in distributed WSNs. Early work on routing in dynamic networks using mobile agents by Kramer concentrated on route discovery using agents to continuously track the network topology and update routing tables at all mobile hosts reached. When a route is requested, an agent is sent to discover routes to the destination. These agents analyze the routing tables on the hosts they arrive at and either return a discovered route to the sender or move on to another machine if no route is found.

Unfortunately, this method increases network load significantly because mobile agents are constantly moving through the network. Other limitations of Kramer's work are that it is difficult to determine the appropriate number of agents to use and it is not possible to have multiple application specific routing algorithms concurrently in use. This system schema is designed to make every node aware of the entire network so that a valid node will not listen to the cheating information from malicious or compromised node which leads to sinkhole attack. The system uses two algorithms. Agent navigation algorithm tells how does a mobile agent

gives network information to nodes and visits every node. Data routing algorithm tells how a node uses the global network information to route data packets. This method has very high overhead if number of nodes are more in WSN. The complexity in storing the information matrix at every node can be decreased in future by using bloom filter technique or some other reduction technique so that it will be a very efficient method.

VI. RELATED WORKS

The survey papers have served as a basic source for gaining the knowledge regarding the various approaches and existing techniques with respect to detection and preventing the sinkhole attack in the Wireless Sensor Networks. A brief report on those existing work is being documented.

Among the existing work which used rules based approach include Krontiris et al [4]. Krontiris used rule based approach to detect sinkhole attack. They create two rules and implanted in Intrusion detection system (IDS). When one of the rules is violated by one of the nodes, the intrusion detection system triggered an alarm but it does not provide node ID of compromised node. The first rule "for each overhead route update packet the ID of the sender must be different your node ID". The second rule "for each overhead route update packet the ID of the sender must be one of the node ID in your neighbors". Also Krontiris et al [4] used the same approaches. There are two rules, the first rule "rule for each overhead route update packet the ID of the sender must be one of node ID in your neighbors". The second rule "for each pair of parent and child node their link quality they advertise for the link between them, the difference cannot exceed 50.

Tumrongwittayapak and Varakulsiripunth [9] proposed a system that used RSSI (Received Signal Strength Indicator) value with the help of EM (Extra Monitor) nodes to detect sinkhole attack. The EM had high communication range and one of their functions is to calculate RSSI of node and send to base station with ID of source and next hop. This process happens instantly when node are deployed. Base station uses that RSSI value to calculate VGM (visual geographical map). That VGM shows the position of each node, then later when EM send updated RSSI value and base station identify there is change in packet flow from previous data this indicate there is sinkhole attack. The compromised node is identified and isolated from the network by base station using VGM value. However, if attack is launched immediately after network deployment, the system will not be able to detect that attack [9]. Also the numbers of EM nodes were not specified for specific number of sensor nodes and the proposed method is focused only on static network.

Chen, et al [1], proposed statistical GRSh (Girshick-RubinShyriaev)–based algorithm for detecting malicious nodes in wireless sensor network. Base station calculates the difference of CPU usage of each node after monitoring the CPU usage of each node in fixed time. Base station would identify whether a node is malicious or not after comparing the difference of CPU usage with the threshold.

Dynamic trust management system was proposed by Roy et al [8] to detect and eliminate multiple attacks such as sinkhole attack. Each node calculates the trust of its neighbour node based on experience of interaction; recommendation and knowledge then sends to base station. The base station decided which node is sinkhole after it received several trust values from other nodes. Therefore the trust value of the node which falls beyond the normal value 0.5 is considered as sinkhole attack [8].

Coppolino and Spagnuolo [2] proposed hybrid Intrusion detection system to detect sinkhole attack and other attacks. They used detection agent which was responsible for identifying sinkhole attack. The hybrid intrusion detection was attached to sensor node and share resource of that node. The suspicious nodes were inserted to the blacklist based on anomalous behavior after analyzed the collected data from neighbors. Then that list is sent to central agent to make final decision based on feature of attack pattern (misused based). Similar to solution proposed by Tumrongwittayapak and Varakulsiripunth [9], it was designed for static wireless sensor network.

Papadimitriou et al [6] proposed a cryptographic approach in routing protocol to address the problem of sinkhole attack. Each node obtained public key which used to verify if the message comes from base station. They also used pair of public and private keys for authentication and sign data message. All keys were uploaded offline before the network was deployed. Their techniques prevented any node to hide its ID and any packet forgery between nodes in the network. This protocol is focused on resistance to sinkhole attack but not to detect and eliminate it.

Fessant et al [10] proposed two protocols which used cryptographic method to increase the resilience of sinkhole attack. Both protocols prevent malicious node from lying about their advertised distances to base station. However, they have not showed the memory usage of their protocols and message size.

CONCLUSION

The increased adaptability of Wireless Sensor Networks in the life style has provided the necessity to improve the security mechanisms adopted in the implemented networks. This paper contains the documentation of the Sinkhole attack which is one among the popular attacks launched in Wireless Sensor Networks, the techniques used to launch the attack, various approaches used to detect and prevent the attack and the mechanisms to overcome the attack.

REFERENCES

[1] 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.

[2] Coppolino, L., D'Antonio, S., Romano, L., and Spagnuolo, G.(2010). An intrusion detection system for critical information infrastructures using WSN technologies. In Critical Infrastructure (CRIS), 2010 5th International Conference on (pp. 1-8). IEEE

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

[4] 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 on Wireless and Mobile Computing, (pp. 526-531). IEEE.

[5] Ngai, E., Liu, J and Lyu, M. (2007), An efficient intruder detection algorithm against sinkhole attack in wireless sensor network. Computer Communications, 30(11), 2353-2364.

[6] Papadimitriou, A., Fessant, L. F. and Sengul, C. (2009). Cryptographic protocols to fight sinkhole attacks on tree based routing in WSN. In Secure Network Protocols, 2009. NPSec 2009. 5th IEEE Workshop on (pp.43-48). IEEE

[7] Pathan, K., AI-S. (2011) Security of Self-Organizing Networks-MANET, WSN, VANET, WMN. ISB N-13:978-1-4398-1920-3. Taylor and Francis Group.

[8] Suman Deb Roy, Sneha Aman Singh, Subhrabrata Choudhury, and N. C. Debnath. (2008). Countering Sinkhole and Black hole Attacks on Sensor Networks using Dynamic Trust Management", In computers and Communications, 2008. ISCC 2008. IEEE Symposium on (pp.537-542). IEEE.

[9] Tumrongwittaya and Varakulsiripunth. (2009). Detection of Sinkhole attack in Wireless Sensor Networks, In ICCAS-SICE, 2009 (pp. 1966-1971). IEEE.

[10] Fessant, F., Papadimitriou, A., Viana, A.Sengul, C. and Polamar, E. (2011) A sinkhole resilient protocol for wireless sensor network: Performance and security analysis. Computer Communications, 35(2), 234-248.

[11] Yanchao Zhang, Wei Liu, Wenjing Lou, Yuguang Fang, "Location-Based Compromise-Tolerant Security Mechanisms for Wireless Sensor Networks", IEEE journal on selected areas in communications, vol. 24, no. 2, February 2006.

[12] A. Cerpa, J. Elson, D. Estrin, L. Girod, M. Hamilton, and J. Zhao, "Habitat monitoring: Application driver for wireless communications technology," in Proc. ACM SIGCOMM Workshop Data Comm. Latin America and the Caribbean, Costa Rica, Apr. 2001, pp. 20–41.

[13] B. Karp and H. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks," in Proc. ACM MobiCom, Boston, MA, Aug. 2000, pp. 243–254.

[14] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," Ad Hoc Netw., vol. 1, no.2, pp. 293–315, 2003.

[15] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: Analysis & defenses," in Proc. 3rd Int. Symp. Inf. Process. Sensor Networks, Berkeley, CA, Apr. 2004, pp. 259–268.

[16] A. Mishra, K. Nadkarni, A. Patcha, "Intrusion detection in wireless adhoc networks," IEEE Wireless Communications, vol. 11(1), pp. 48-60, Feb. 2004.

[17] Daniel Dallas, Christopher Leckie, Kotagiri Ramamohanarao, "Hop-Count Monitoring: Detecting Sinkhole Attacks in Wireless Sensor Networks", 1-4244-1230-7/07/_2007 IEEE.

[18] Hairong Qi, Yingyue Xu, Xiaoling Wang, "Mobile-Agent- Based Collaborative Signal and Information Processing in Sensor Networks," in Proceeding of the IEEE, Vol. 91, NO. 8, pp.1172-1183, Aug. 2003.

[19] Wu, Q., Rao, N.S.V., Barhen, J., etc, "On computing mobile agent routes for data fusion in distributed sensor networks," IEEE Transactions on Knowledge and Data Engineering, Vol.16, NO. 6, pp. 740-753, June 2004.

[20] S. Capkun, L. Buttyan, J. Hubaux, SECTOR: Secure Traking of Node Encounters in Multi-hop Wireless Networks, in: proc. Of SASN 2003. Fairfax, Virginia, October 2003.

[21] K.N. Ross and R.D. Chaney, "Mobile Agents in Adaptive Hierarchical Bayesian Networks for Global Awareness," Proc. IEEE Int'l Conf. Systems, Man, and Cybernetics, pp. 2207-2212, 1998.

[22] Hairong Qi, Iyengar, S., Chakrabarty, K., "Multiresolution data integration using mobile agents in distributed sensor networks," IEEE Transactions on Systems, Man and Cybernetics, Vol.31, No.3, pp. 383-391, Aug. 2001
[23] Teng, L., and Zhang, Y. (2010). Secure Routing Algorithm against Sinkhole attack for Mobile Wireless Sensor Network, In Computer Modeling and Simulation, 2010. ICCMS'10. Second International Conference on (Vol. 4 pp.79-82). IEEE.
[24] I.Akyildiz, W.Su, Y.Sankarasubramaniam, E.Cayirci, Wireless sensor networks: a survey, Computer Networks 38 (4) (2002) 393–422.
[25] A.Perrig, J.Stankovic, D.Wagner, Security in wireless sensor networks, Communications of the ACM 47 (6) (2004) 53–57.
[26] H.Chan, A.Perrig, Security and privacy in sensor networks, Computer 36 (10) (2003) 103–105.
[27] C.Karlof, D.Wagner, Secure routing in wireless sensor networks: Attacks and counter measures, AdHoc Networks 1 (2) (2003) 293–315.
[28] R.Villalpando, C.Vargas, D.Munoz, Network coding for detection and defense of sinkholes in wireless reconfigurable networks, in: Proceedings of International Conference on Systems and Networks Communications, 2008, pp.286–291.
[29] B.Choi, E.Cho, J.Kim, C.Hong, J.Kim, A sinkhole attack detection mechanism for LQIbased mesh routing in WSN, in: Proceedings of International Conference on Information Networking, 2009, pp.1–5.
[30] I.Krontiris, T.Giannetsos, T.Dimitriou, Launching a sinkhole attack in wireless sensor networks; the intruder side, in: Proceedings of IEEE International Conference on Wireless and Mobile Computing, 2008, pp.526–531.

