International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
DOI: https://doi.org/10.17762/ijritcc.v10i7.5562
***Article Received**: 05 May 2022 **Revised**: 30 May 2022 **Accepted**: 20 June 2022 **Publication**: 31 July 2022*

A Scheme for Detecting the Sinkhole for Secured WSN

Poornimha.J[1], A V Senthil Kumar[2]
[1]Assistant Professor, Department of Computer Science, KG College of Arts and Science Coimbatore-641035, India
[2]Professor and Director, Department of Computer Applications, Hindusthan College of Arts and Science, Coimbatore-641004, India.

Abstract:
Because of the limited computation capability as well as transmissions being broadcasted in a wireless sensor network (WSN) they are supposed to be more susceptible for attacks related to the security. As present wireless sensor networks have low-power constraints as well as increased complexity, thus for nodes' performance analysis related to the embedded software and network simulation efficient approaches are required. Additionally, as these networks are used to deal with the sensitive information and operated in the adverse unattended environments, thus, security feature must be added in most of these wireless sensor networks. In this paper a novel scheme for detecting various sinkhole nodes for wireless sensor network (WSN). The results of this proposed scheme show the 1.75% fake positive rate and 96% of detection rate. In comparison to the previous schemes, these aspects are considerably better. In addition to these aspects, our scheme also achieves the communication as well as computational efficiencies. As a result of which, this proposed scheme proved to have better results in many applications.

Keywords: *Security, Key management, Authentication, Sinkhole attack, WSN.*

1. INTRODUCTION

There is an increase deployment of smart environments in the transportation, industrial, ecological, health, military, building applications and many more. Generally, smart devices are used in such environments which acquires data from actual world, process it and then communicates the data into information processing centers, where few information-based services are generated. Wireless Sensor Networks provides the smart environments with the information they uses which is generally used for recording as well as monitoring the environmental and physical conditions along with this, collected data is communicated to a base station. Such Wireless Sensor Network is considered as a spatially distributed sensing nodes (devices) group that are self-powered [3]. These sensor are capable of processing as well as communicating data and are small in size. With the help of sensor nodes environment's ambient conditions are measured, which are then transformed into electrical signals and sent to sink through radio transceiver and after that a gateway is used to send back the aggregated information to a base station [40].

In a WSN as in Figure 1, various sensors are dispersed in a particular area for monitoring conditions such as pollutants, pressure, vibration, sound, and temperature etc. The digital data network as well as physical world is linked with the WSN and results in providing a distributed network with limitations of energy efficiency lifetime and, scalability[1]. Initially, the development of WSN is for purpose of disaster rescue and military but due to the ISM band (2.4 GHz) availability, public applications are being developed with this technology [17].

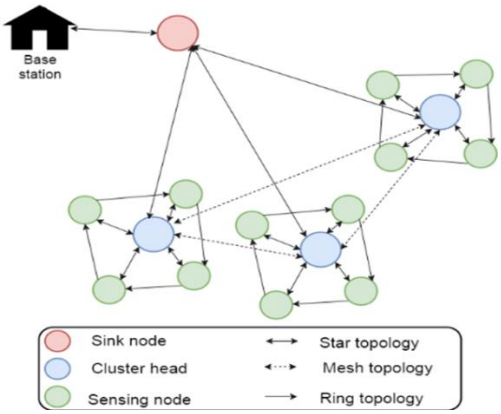

Figure 1 Wireless Sensor Network

Security and connectivity are two significant considerations during the WSN deployment. WSN is considered as connected when base node and other sensor nodes are connected with a physical (wireless) communication path with one another. Generally, data forwarding is done through multi-hop paths where process is dependent on intermediate sensor nodes. Furthermore, for a secure WSN, each communication path should have a pair-

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
DOI: https://doi.org/10.17762/ijritcc.v10i7.5562
***Article Received**: 05 May 2022 **Revised**: 30 May 2022 **Accepted**: 20 June 2022 **Publication**: 31 July 2022*

wise secret key for encrypting each communication [21]. Primarily, secure WSN is focused in this paper and is explained in following sections.

1.1 WSN Security Analysis

The sensor nodes are very vulnerable to various attacks because of the WSN's simplicity along with the limited resources. Radio transmission can be eavesdropped, new bits can be injected in channel, previously heard packets can be replayed by the attacker. For WSN security, all security properties of the network must be supported which includes: availability, authenticity, integrity, and confidentiality. Some malicious nodes can be deployed by the attacker that has the same hardware capabilities as that of normal nodes which then attack the system accordingly. These malicious node can be separately purchased by the attacker, or actual nodes can be captured and their memory is overwritten physically[9].Additionally, there are situations in which attacking nodes consists of high-quality communications links through which attack is coordinated. It has been noticed that these sensor nodes are not resistant to tempering so in case of node compromization, node's data, code, key material can be extracted. Significant per-unit cost is added in case of extremely effective tamper resistance, whereas these sensor nodes are not that much expensive [20][24][25][26]

Security Goals for Wireless Sensor Networks

In most of the cases, security is considered as the system architecture's standalone component or in some cases there exists a separate component that provides security. Although, the later approach is considered as network security's flawed approach. For achieving a secure system, it is required that each component must be integrated with security. Furthermore, in most of the situations, where components are not integrated with the security at times of system development design resulted in point of attack. It results in the fact that system design's each aspect must be pervaded by the security [8].

For the sensor networks' unique constraints' security goals as well as traditional networks some security goals [34][35][36] are comprised which are as follows:

- *Confidentiality*

It checks the messages concealment ability so that messages that are communicated through the sensor network will be confidential from a passive attacker. Typical WSN are utilised in environments where highly

confidential as well as sensitive data is being distributed. Sensor networks should not disclose sensor readings and information to other networks. An example of the need for confidentiality is the use of a wireless sensor network in an emergency medical situation. Patient information being transmitted to caregivers via nodes should maintain be kept private and confidential. The key to achieving confidentiality in these protocols is to implement symmetric key authentication and encryption. It guarantees that data secrecy is provided with the data encryption and only intended receivers possess the information and will decrypt it.

- *Integrity*

Integrity means the capability of network that confirms that there is no tampering, alteration as well as changes in the message when they were on network. The data reliability is confirmed by the integrity. For data communication and transmission, one of the important requirement is data integrity. However, it is very difficult to achieve. Receiver has been ensured that the data he/she received is not changed in any way by an adversary in its transit. This is very difficult to detect without authentication of the data.

- *Authentication*

It verifies the message reliability by message's origin identification. Sender's identity is verified by data authentication. In sensitive situations and more importantly in situations where decisions are being made based on transmitted data, authentication is pertinent. With data authentication, sender is authenticated by the receiver. It is important because an attacker can insert messages into the network easily. This is considered one of the most common forms of attacks. The receiver must be able to identify the sender as well as ensure that the data is valid before operating on that data. Achieving data authentication can be done with symmetric key mechanisms in two party communications. This is simply a network where the two parties share a single secret key for passing messages. Only when the correct key is transmitted do they accept messages. This does not work for broadcast settings and were multiple notes and base stations are in play. If all nodes are sharing the same secret key and you only want a single node to receive the message it is not secure. Any of the nodes who know the secret key have direct access to that data. The way to defend this is to use an asymmetric key authentication.

- *Availability*

It verifies the capability that resources can be used in spite of availability of network for communicating messages. The reason WSN exist to achieve communication among BS and nodes in an efficient and timely manner. Communication of data is not efficient if it is not fresh, meaning recent and no attacker played old messages again. 2 freshness types are there, which are: strong-freshness and weak-freshness. Their definitions are somewhat implied, but delayed estimation as well as total order is provided by strong freshness, and no

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
DOI: https://doi.org/10.17762/ijritcc.v10i7.5562
Article Received: 05 May 2022 Revised: 30 May 2022 Accepted: 20 June 2022 Publication: 31 July 2022

delay information is carried by weak-freshness but partial message ordering is provided.

The WSN may face some serious attacks that consists of hole attacks like blackhole, sinkhole, greyhole, wormhole, etc. When these attacks are presented in the WSN, it results in delayed reception of information at destination, and sometime intended information is modified or lost as well as high energy expenditure is also caused [6][10][13][15][18][27]

Grayhole Attack

It is considered as the blackhole attack's variation where packets are dropped with certain probability or selectively by the malicious attacker. A specific node is used by attacker for dropping packets and then these packets are sent to other nodes. Also, traffic type may be used as basis for dropping packets, for instance, all TCP (Transmission Control Protocol) packets can be forwarded while UDP (User Datagram Protocol) packets will be dropped [12], [13], [14]. Several network performance parameters like EED and throughput can be affected by the grayhole, blackhole, and wormhole nodes presence in WSN.

Wormhole

Received messages are channelled by the attacker to network's one part above low latency link and then this message is replayed in network's other parts, in a wormhole attack [39]. Generally, attacker is presented in a closed proximity to BS from where it can easily interrupt the routing process by introducing the wormhole. All the normal nodes are convinced by the adversary that via the wormhole route they are just 1-2 hop away from the BS but actually there exists multiple hops to the BS. It resulted in creating the sinkhole: as a high-quality route is artificially provided to the BS by the adversary on wormhole's other side, thus all the traffic will be attracted towards this because it seems to be more attractive.

Sinkhole

For introducing a sinkhole attack in a network, there exists 2 ways: a fabricated node is introduced to the network or network's node is hacked[11]. After that, malicious node attempts to lure the traffic towards itself by promoting that it has the shortest route to BS. Due to this every node is lured towards the sinkhole along with the nodes that are actually near to BS than sinkhole node.[22] It results in alteration of data by the sinkhole or intruder node and thus network security is compromised as in Figure 2.

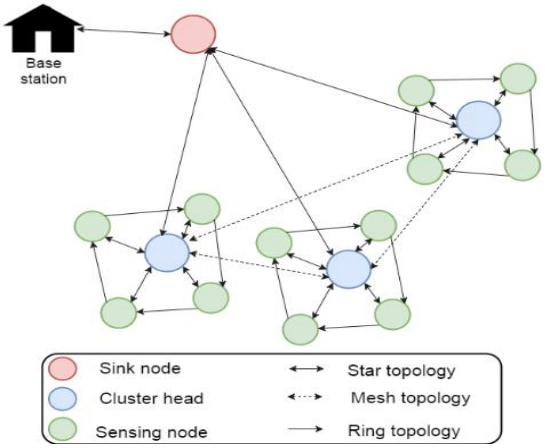

Figure 2 Sinkhole Attack

There are two ways for initiating the sinkhole attack: either from outside the network or from inside of the network. Outside the network: a direct route is formed to BS by the intruder through itself by luring other nodes to route their data via this node. Inside the network: intrusion is begun by a bugged node that is used by the attacker.

On successful deployment of sinkhole attack, three possibilities arise: message can be modified, message can be delayed, or message can be lost or attacker node drops the message [16, 17, 21]. Depending on these possibilities, sinkhole attacker node is of three types:

- SDL (Sinkhole message delay) nodes: Message forwarding is delayed due to sinkhole attacker nodes.
- SDP (Sinkhole message dropping) nodes: Messages are dropped by the sinkhole attacker nodes, and sometimes there will be selective dropping of messages.
- SMD (Sinkhole message modification) nodes: Messages are modified by the sinkhole attacker nodes before messages are forwarded to next node.

1.2 Threat model

In this proposed scheme famous Dolev-Yao threat model is used [25], where in an insecure channel, any 2 communicating nodes can communicate [37]. Similar threat model is used in this scheme, where the communicating nodes are not reliable as well as channel is insecure. The message can be dropped, modified, or lost when a sinkhole attacker node is present in the WSN, which then affects network performance seriously like high EED, throughput reduction and PDR (Packet Delivery Ratio) reduction. Furthermore, it has been assumed that in a network CH or some sensor nodes can be physically captured by an attacker and then by using

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
DOI: https://doi.org/10.17762/ijritcc.v10i7.5562
Article Received: 05 May 2022 Revised: 30 May 2022 Accepted: 20 June 2022 Publication: 31 July 2022

node's information, malicious nodes can be deployed in the network by the attacker which then act as sinkhole attacker node.

1.3 Organization of problem

WSNs sinkhole attack detection schemes proposed by various researchers has been reviewed.

Du *et al.* [28] presented an efficient and secure routing protocol for heterogeneous sensor networks. Particularly they used high-end sensors that are powerful. At time of experiment, they noticed that in comparison to the existing directed diffusion techniques better routing performance is achieved by the proposed routing protocol. When the failure nodes increased, it results in decreasing the proposed scheme's delivery ratio. Furthermore, when there are great L-sensors numbers it results in better delivery ratio that reduces significantly when L-sensors are less in number.

Hamedheidari *et al.* [13] presented a defensive mechanism which is dependent on mobile agent against sinkhole attack. A three-step negotiation is used for informing the sensor nodes by its neighbors by mobile agents that helps sensor nodes to ignore the traffic that is caused by the malicious sinkhole attacker nodes. When this scheme is evaluated on its performance, the evaluation is made for throughput, packet loss rate, mobile agent energy consumption, etc. For WSN, this scheme has a drawback that network overhead is increased due to mobile agents' use.

For protecting WSN from sinkhole attack Krontiris *et al.* [23] presented an intrusion detection system. For sinkhole attack's successful detection, IDS systems are embedded as well as designed with few rules. Although, low DR has been observed in their proposed scheme.

Salehi *et al.* [12] presented a sinkhole attack detection mechanism. This algorithm initially classifies a suspected node group and after that depending on the network flow information, there is confirmation of sinkhole attacker nodes. The proposed scheme's effectiveness is checked by performing simulations. Furthermore, low DR has been observed in their proposed scheme.

Shafiei *et al.* [20] presented an approach for identifying sinkholes (energy holes). A centralized model is used for detecting the sinkhole attacker node. Also, for eliminating these nodes a lightweight mitigation approach is also presented.

For a cluster based WSN an IIDS (Integrated Intrusion Detection System) is presented by Wang *et al.* [16]. With the network data's real-time analysis, this propose approach can avoid attack. There are 3 IDS's I the proposed scheme like MIDS (Misuse Intrusion Detection System), HIDS (Hybrid Intrusion Detection System), and IHIDS (Intelligent Hybrid Intrusion Detection System). Misuse as well as anomaly detection modules is used for detection that provides low false positive (FP) rate with high detection rate (DR).

Zhang *et al.* [7] presented a redundancy mechanism from preventing from sinkhole attack. Suspicious nodes were sent messages from various paths, in this technique. Depending upon the suspicious nodes' replied messages, it helps in identifying the sinkhole attacker nodes. Particular scheme's effectiveness is tested using NS2 tool by performing simulations.

Onat and Miri [31] and Da Silva et al. [30] both proposed IDS systems that are similar, in which in the network, there exists some monitoring nodes that keeps a watch on their neighbour nodes so as to check for attackers. Messages in a specific radio range are listened by these nodes and then stored in a buffer which is then used by IDS system. In such systems, monitoring nodes are not collaborated in any way. It has been discovered that one of the significant factor is buffer size which is involved in false alarms rate.

For cluster-based WSN a lightweight IDS is proposed by Hai *et al.* [19]. Also, for minimising the network's triggered intrusion modules an algorithm is presented by utilising for reducing the sending packet alert. With the help of such approach, WSN's most routing attacks can be detected. It has been discovered at times of experiment that in comparison to the existing techniques, less energy consumption is needed by this technique. Although, higher FP rate is observed by this technique.

Initially, Ngai et al. [29] proposed a method for sinkhole attacks detection that involves the base station thus, protocol's communication cost is increased due to such detection process. Base station floods the network with a request message that includes the influenced nodes' IDs. BS receives a message from the affected node that contains node ID, next hop ID and the cost associated with it. After that, BS uses this information in building a network flow graph which helps in sinkhole identification.

A mechanism has been proposed by Wood et al. [26] for mapping and detecting the jammed areas. A mapping protocol is described by them for the nodes through which jammer is surrounded. With the help of such configuration network applications are allowed to reason region to be considered as an entity instead of a group of congested nodes and broken links.

A packet leash mechanism is proposed by the Perrig et al. [38] which detects as well as defends against wormhole attack. Leash can be considered as geographical or temporal information which is attached to the packet so that maximum transmission distance of packet is restricted.

Chen et al [18] presented an algorithm that detects sinkhole attack for larger WSN that are dependent on the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
DOI: https://doi.org/10.17762/ijritcc.v10i7.5562
Article Received: 05 May 2022 Revised: 30 May 2022 Accepted: 20 June 2022 Publication: 31 July 2022

network nodes' CPU usage. CPU usage is monitored by every node and then data usage is reported to the BS periodically. Here, each node's CPU usage difference is calculated by the base station. A threshold value is used for difference comparison, and then it has been identified by the base station that whether a node is malicious or not. This approach also resulted in high traffic overhead.

A SEF (Statistical En-route Filtering) mechanism is proposed by Ye et al. [33] for false report dropping and detection. This mechanism utilises data filtering, probabilistic verification, and multiple authentication codes for determining each report's truthfulness.

In our scheme we have focused on the sinkhole attacks, in which one-to-many data communications are actively disturbed by the multiple malicious nodes as well as by the intruder.

Also, packet leash is introduced by Hu et al. [32] that reveals each packet's distance and maximum transmission time. An assumption is made that a key is obtained by each node for any other node as well as every data packet is provided with authentication. On the other hand, in proposed scheme neither each data packet's authentication nor promiscuous mode support is provided by the node[4]. Existing protocols technique used and their drawbacks are summarized in Table 1.

Author	Technique used	Drawbacks
Zhang et al. (2014)	Redundancy mechanism	low *DR*
Shafiei et al. (2014)	Geostatistical hazard model used for estimation of sink holes	network congestion areas can have some issues due to energy expenditure maps which affects FPR as well as DR
Hamedheidari et al. (2013)	Detection based on Mobile agent	Network overhead is high
Salehi et al. (2013)	Detection based on network information flow and suspected nodes' grouping	High *FPR*
Wang et al. (2013)	Uniformly and Gaussian distributed WSN	less number of nodes with low *DR*
Wang et al. (2011)	misuse IDS approaches, for CH HIDS and for the sink IHIDS is used	Higher computational cost and low *DR*
Krontiris et al. (2008)	Neighbor lists are intersected for cooperative detection	low *DR*
Wang et al. (2008)	Detection based on single and multi-sensing	low *DR*
Du et al. (2007)	TTSR (Two Tier Secure Routing)	less L-sensors number with very low PDR

Table 1: Existing protocols technique used and their drawbacks.[22]

Proposed cluster-based scheme for detecting sinkhole nodes is described in section 2. Mathematical analysis is provided in section 3. Simulation parameters as well as results using NS2 are provided in the section 4 with the help of security analysis. Finally, the paper is concluded in section 5.

2. PROPOSED SCHEME'S MATHEMATICAL MODEL

For our scheme mathematical model is developed in this section for complete network in terms of EED, throughput and PDR.

2.1 End-to-end delay

Let end-to-end delay under our proposed scheme, under sinkhole attack, and under normal flow be Δs, Δa, and Δn, respectively. The end-to-end delay in normal flow is represented as

$\Delta \boldsymbol{n} = \Delta,$

Where, Δ is represented as

$$\Delta = \frac{\sum_{i=1}^{p}(T_{rec_i} - T_{send_i})}{p},$$

p represents packet's total number and *Tsendi* and *Treci* represents i^{th} packet's sending and receiving time. Furthermore, estimation of EED in sinkhole attack is calculated as:

$$\Delta_a = \Delta_{n'} + (\Delta_{n_{sdpa}} + \Delta_{n_{sdla}}),$$

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
DOI: https://doi.org/10.17762/ijritcc.v10i7.5562
Article Received: 05 May 2022 Revised: 30 May 2022 Accepted: 20 June 2022 Publication: 31 July 2022

where *n* represents network's sensor nodes, *nsdpa* represents SDP number and *nsdla* represents SDL number in that cluster, *n*0 = *n* – (*nsdpa* + *nsdla*), *nsdpa* represents the delay corresponding to *nsdpa* SDP, and *_nsdla* the delay corresponding to *nsdla* SDL. Lastly, end-to-end delay in this proposed scheme is represented as

$$\Delta s = \Delta n0 + (\Delta FNsdpa + \Delta FNsdla),$$

where *FNsdpa* represents the normal nodes as detected by the proposed scheme, which are SDP, *FNsdla* represents normal nodes as detected by the proposed scheme, but are SDL, *n*00 = *n*–(*nFNsdpa*+ *nFNsdla*) the normal nodes under our scheme, Δ*FNsdpa* represents *FNsdpa* nodes corresponding delay and Δ*FNsdla* the *FNsdla* nodes corresponding delay.

2.2. Throughput

Let network throughput under our proposed scheme with sinkhole attack, and with normal flow is represented by *THs*, *THa*, and *THn*, respectively. Furthermore, delivery time of packets under our proposed scheme, under sinkhole attack, and under normal flow is represented as *Ts*, *Ta*, and *Tn* respectively. Thus, throughput under normal flow is represented as

$$THn = |Md0| \_ |pkt| Tn$$

Likewise, the estimation of throughput during attack is as:

$$THa = |pkt| \_ (|Md0| - (|Mdsdpa| + |Mdsdla|)) Ta$$

also, the throughput is presented as:

$$THs = |pkt| \_ (|Md0| - (|Md1| + |Md2|)) Ts,$$

where |*pkt*| represents the data packet size.

2.3. Packet delivery ratio

Let PDR under our proposed scheme, under sinkhole attack, and under normal flow is represented by *PDRs*, *PDRa*, and *PDRn* respectively. Furthermore, |*Md*| represents the data packets number that cluster members send, and |*Md*0 | represents data packets number that CH receives. Moreover, |*Mdsdpa*| represents SDP dropped data packets number in network, |*Mdsdpa*0| represents SDP nodes dropped data packets number as true positives (TP) as well as |*Md*1| represents SDP nodes dropped data packets number as false negative (FN). Furthermore, |*Mdsdla*| represents *SDL* nodes delayed data packets' total number in network, |*Mdsdla*0| *SDL* nodes delayed data packets' total number (TP) as well as |*Md*2 | *SDL* nodes delayed data packets' total number (FN)

Thus, |*Md*1| = |*Mdsdpa*|– |*Mdsdpa*0 | and |*Md*2| = |*Mdsdla*| – |*Mdsdla*0 |. Then, under the normal flow, we have,

$$PDRn = \frac{|Md0|}{|Md|}$$

Furthermore, estimation of PDE during sinkhole attack is as:

$$PDRa = |Md0| - (|Mdsdpa| + |Mdsdla|) |Md|$$

Lastly, estimation of PDR is as:

$$PDRs = |Md0| - (|Md1| + |Md2|) |Md|$$

3. PROPOSED SCHEME ANALYSIS

Proposed scheme's security is analysed in this section. Furthermore, cluster's computational overheads and communication is also analysed.

3.1 Security analysis

Every cluster consist of a CH (Cluster Head) which is a powerful node. In a corresponding cluster, all SDL, SDP, and SMD nodes are detected by the cluster head. A new CH deployment is required if an attacker compromised the current cluster head and base station detects it. The information regarding every members' remaining battery backup as well as identities is in the cluster head.

There exists 3 types of sinkhole attacker nodes namely, SDP, SDL, and SMD nodes depending on the fact that there is a successful deployment of the sinkhole attacker node and it has initiated the data tampering which means unnecessary delays are caused along with dropping as well as modifications. With the help of our scheme, all these three nodes can be detected at the same time. This scheme's working has 2 phases. Phase 1: Sinkhole node existence algorithm is used for detecting the sinkhole attacker node's existence that utilises the parameters like nodes' remaining energy, suspected node's coefficient, hop count for source to destination path information and node identification. Some conditions should be met for detecting the sinkhole attacker node.

After phase 1 completion, all sinkhole attacker nodes list is obtained that contains SDL, SDP and SMD nodes. The list specifying the attacker node does not specifies the nodes' types. In phase 2, sinkhole node identification algorithm is used for the detecting the node types. HMAC is used by the CHj cluster head for identification of SMD nodes. Consider a situation where a message is received by the cluster head which is a sinkhole node and the message received is different from the original message that source node has sent. Such situation, results in difference in original message and received message's HMAC values. Furthermore, in this situation it has been confirmed by the cluster head that sinkhole node is a SMD node.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
DOI: https://doi.org/10.17762/ijritcc.v10i7.5562
Article Received: 05 May 2022 Revised: 30 May 2022 Accepted: 20 June 2022 Publication: 31 July 2022

If any kind of message delay is there by some sinkhole attacker node which is observed by cluster head as original message receiving time is less than current message's receiving time. Thus, factors like network congestion is also checked by the cluster head. The node is a SDL node, when no congestion is there. In case, there is no message from sinkhole node to the cluster head, then node is checked that either it is SDP node or network has some more issues like failure of node. The node receives a status data query message and every time there is increment in waiting time. If cluster had not received a message in response or the data message in specified waiting time from sinkhole node, then node is considered to be failed. Furthermore, node is detected as SDP node if cluster head received the response message but not the data message. Thus, in detection process phase 2 different sinkhole attacker nodes types are identified.

3.2 Communication cost

For computing the communication cost, it has been assumed that a cluster is consist of n sensor nodes. Cluster members receives n status-data query messages from cluster head in normal flow. After that cluster head receives n status reply messages from its members as well as data messages is also sent to cluster head. Thus, during the normal flow, the exchanged messages between cluster head and its members is 3n. At sinkhole attack, no data messages is sent from the sinkhole dropping nodes, thus cluster head only receives data messages.

In the proposed scheme, when data messages are not received from SDP nodes by the cluster head, then in response SDP node receives more status-data query messages from cluster head. Furthermore, no data message is sent in response to that but cluster head receives status reply messages only. After detection's both phases,
sinkhole attacker node as well as their type is identified by the cluster head. Cluster members are alerted by the cluster head by sending them information messages. Whereas, SDL, SDP and SDM nodes does not receives these information messages from cluster head. Therefore, under the proposed scheme, the total exchanged messages are given by

$$[n + n + (n - nsdp) + nsdp + nsdp + n - (nsdm + nsdp + nsdl)] = 4n - (nsdm + nsdl).$$

3.3 Computation cost

There are two phases in the proposed detection scheme. Phase 1: sinkhole node existence algorithm is used for detecting sinkhole attacker node's presence in the network. In case of confirmation of sinkhole node, sinkhole node identification algorithm is executed for identifying the sinkhole node in the phase 2. Therefore, firstly, sinkhole node existence algorithm is performed and after that sinkhole node identification algorithm is run.

During phase 1: AODV (ad hoc on demand distance vector) routing protocol mechanism is used by cluster head for finding the various paths that requires O (2d) time, in which d represents cluster's network diameter[2]. Furthermore, d can also be expressed as n available sensor nodes and m edges in a cluster. The sinkhole node existence algorithm's remaining steps executes in a linear time. Thus, sinkhole node existence algorithm's complexity is denoted as O (n^2). Furthermore, sinkhole node identification algorithm is executed in O (n) time.

4. SIMULATION

Our proposed scheme's practical perspective is presented in this particular section. The network simulator NS2 version 2.35 is used for performing the simulations. For performing the network's discrete event simulation, NS2 software is used. For networking research, this software is being used regularly. Over wireless and wired networks various multicast protocols, routing protocols (e.g., DSR, AODV etc.) and TCP/UDP protocols simulation support is provided by the NS2. In research community, NS2 is considered as standard experiment environment. [5].

4.1 Simulation environment

Our scheme is simulated using NS2 simulator on Ubuntu 14.04 LTS platform. Simulation area used is 650 × 250 m^2. 100 nodes are deployed in the deployment area so that in every cluster there will be 9 sensor nodes and 1 cluster head. Simulation parameters are represented in Table 2.

Parameters	Description
Platform	Ubuntu 14.04 LTS
Deployment area	650 × 250 m^2
Network Topology	Tree
Network Size	100 nodes
Total Clusters	10
Total Cluster Heads	10
Sensor Nodes in Each cluster	9
Attacker Nodes	20
Simulation time	1800 seconds
Traffic Type	CBR/UDP
Size of Packet	512 bytes
Transmission rate of Packet	25 kbps
Routing Protocol	AODV
MAC type	IEEE 802.11
Clustering Method	Static
Sensor's Communication Range	25m
CH's Communication Range	50m

Table 2: Simulation Parameters

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
DOI: https://doi.org/10.17762/ijritcc.v10i7.5562
Article Received: 05 May 2022 Revised: 30 May 2022 Accepted: 20 June 2022 Publication: 31 July 2022

4.2 Simulation scenarios

The WSN is simulated in network simulation under proposed detection scheme, under sinkhole attack, and under normal flow.

4.2.1 Network scenario under normal flow.

Under the normal flow network scenario contains 100 nodes are deployed in the deployment area and divided into 10 clusters so that in every cluster there will be 9 sensor nodes and 1 cluster head.

4.2.2 Network scenario under sinkhole attack.

Under the normal flow network scenario contains 100 nodes are deployed in the deployment area and divided into 10 clusters so that in every cluster there will be 9 sensor nodes and 1 cluster head. 20 sinkhole attacker nodes were considered. Thus, in the network 20% nodes are considered as sinkhole attacker nodes.

4.3 Results and discussion

Following network statistics are computed in the simulation.

- Throughput (in kbps)
- End-to-end delay (EED) (in ms)
- Packet delivery ratio (PDR), (ii)

4.3.1 Impact on throughput

Throughput can be explained as actual bits transferred per unit time. The throughput calculated under proposed scheme is 7.45 kbps, under sinkhole attack it is 3.41 kbps and under the normal flow it was calculated to be 8.05 kbps. Therefore, it can be clearly observed that in comparison to the sinkhole attack, there is a significant improvement by our proposed scheme is shown in Figure 3.

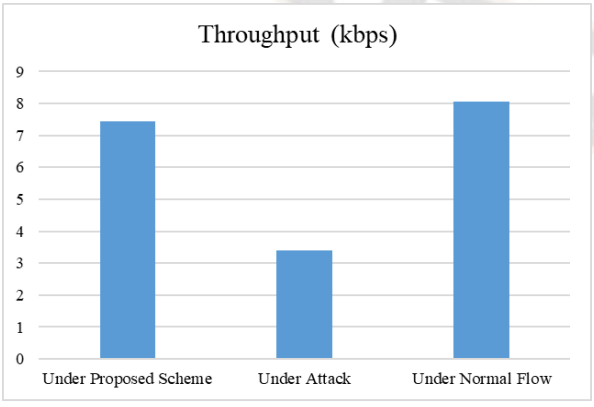

Figure 3 Throughput

4.3.2. Impact on end-to-end delay

The end-to-end delay is expressed as average time used by data packet to reach the base station. The end-to-end delay calculated under proposed scheme is 95.34 ms, under sinkhole attack it is 609.75 ms and under the normal flow it was calculated to be 78.75 ms. Therefore, it has been clearly seen in figure 4 that in our proposed method delay time decreases.

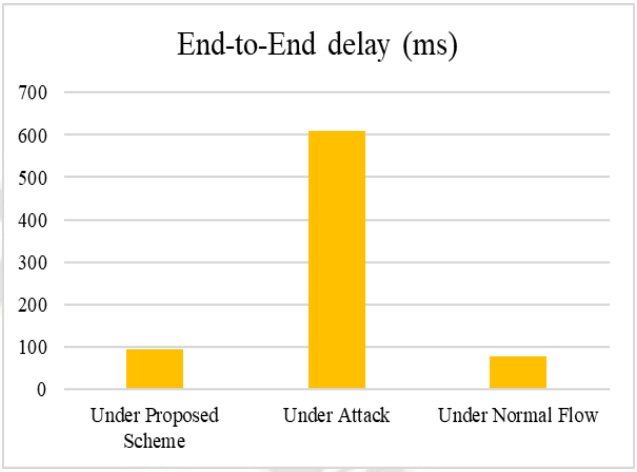

Figure 4 End to End Delay

4.3.3 Impact on packet delivery ratio

PDR (Packet delivery ratio) can be expressed as ratio of packets received at base station to the packets that source node has sent. The PDR calculated under proposed scheme is 0.89, under sinkhole attack it is 0.45 and under the normal flow it was calculated to be 0.89. Therefore, it can be clearly observed that in comparison to the sinkhole attack, there is a significant improvement of PDR in our proposed scheme as shown in figure 5.

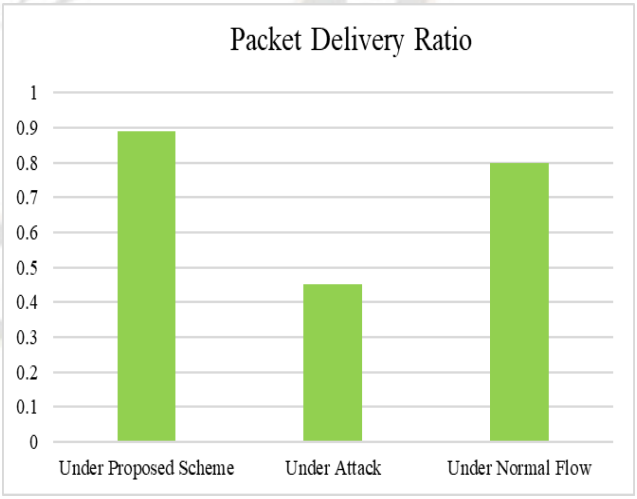

Figure 5 Packet Delivery Ratio

Lastly, Table 3 shows the network statistics of our scheme.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
DOI: https://doi.org/10.17762/ijritcc.v10i7.5562
Article Received: 05 May 2022 Revised: 30 May 2022 Accepted: 20 June 2022 Publication: 31 July 2022

Parameters	Under Proposed Scheme	Under Attack	Under Normal Flow
Throughput (kbps)	7.45	3.41	8.05
End-to-End delay (ms)	95.43	609.75	78.75
Packet Delivery Ratio	0.89	0.45	0.80

Table 3: Network statistics summary

Furthermore, through the simulation there were following explanations:

- With our proposed scheme, according to confusion matrix, there is detection of 8 SDL nodes, 5 SDP nodes and 6 SMD nodes.
- Also, our network consists of 80 normal nodes as well as 20 sinkhole attacker nodes.

5. CONCLUSION

WSN performance can be seriously affected by the various sinkhole attacker nodes. As discussed in the literature section, the existing approaches have some limitations and are not as efficient as required. Therefore, a novel detection technique has been proposed in this paper for sinkhole nodes detection in wireless sensor networks. Network performance is rapidly degraded by the various sinkhole attacker nodes presence. During the sinkhole attack, there is decrease in the throughput from 8.05 kbps to 3.41 kbps, increase in end-to end delay from 78.75ms to 609.75ms as well as decrease in PDR is noted from 0.80 to 0.45. Thus, it is important that for the sinkhole attack a detection scheme must be there.

The proposed scheme results in significant improvement of network performance parameters. During the proposed scheme deployment, there is increase in throughput to 7.45 kbps, decrease in end-to-end delay to 95.43 ms and increase in PDR to 0.89. Furthermore, there is minimum message exchanges in our proposed scheme that resulted in decreasing of the communication cost. In comparison to the resourceful cluster heads lesser computation and communication overheads are required by the proposed scheme. Moreover, this proposed scheme is highly secured from the sinkhole attack. Thus, this scheme can be beneficial for sensor nodes that are restricted due to energy resources as well as lower computation and communication overheads in comparison to existing techniques.

6. REFERENCES

[1]. Poornimha, J., Senthil Kumar, A.V., Abdullah, H.M.A."A New Approach to Improve Energy Consumption Time and Life Time using Energy Based Routing in WSN" 2021, IEEE International Conference on Emerging Trends in Industry 4.0, ETI 4.0 2021, 2021.

[2]. Poornimha.J, A.V.Senthil Kumar, "An enhanced design of AODV protocol to increase the energy consumption in the MANET.", International Journal of Research,2019, ISSN NO:2236-6124 .

[3]. Diaz, Alvaro, and Pablo Sanchez. "Simulation of attacks for security in wireless sensor network." Sensors 16.11 (2016): 1932.

[4]. Wazid, Mohammad, et al. "Design of sinkhole node detection mechanism for hierarchical wireless sensor networks." *Security and Communication Networks* 9.17 (2016): 4596-4614.

[5]. Deepak Mathur, N. K. V. . (2022). Analysis & Prediction of Road Accident Data for NH-19/44. International Journal on Recent Technologies in Mechanical and Electrical Engineering, 9(2), 13–33. https://doi.org/10.17762/ijrmee.v9i2.366

[6]. Wang J. NS-2 Tutorial. Available at http://www.cs.virginia.edu/~cs757/slidespdf/cs757-ns2-tutorial1.pdf. Accessed on March 2015..

[7]. Shafiei H, Khonsari A, Derakhshi H, Mousavi P. Detection and mitigation of sinkhole attacks in wireless sensor networks. *Journal of Computer and System Sciences* 2014; **80**(3): 644–653.

[8]. Zhang FJ, Zhai LD, Yang JC, Cui X. Sinkhole attack detection based on redundancy mechanism in wireless sensor networks. *Procedia Computer Science* 2014; **31**: 711–720.

[9]. Shafiei H, Khonsari A, Derakhshi H, Mousavi P. Detection and mitigation of sinkhole attacks in wireless sensor networks. *Journal of Computer and System Sciences* 2014; **80**(3): 644–653.

[10]. Oreku, George S. "Reliability in WSN for security: Mathematical approach." 2013 international conference on computer applications technology (ICCAT). IEEE, 2013.

[11]. Wazid M, Katal A, Sachan RS, Goudar RH, Singh DP. Detection and prevention mechanism for Blackhole attack inWireless Sensor Network. *International Conference on Communications and Signal Processing (ICCSP 2013)*, Coimbatore, India, 2013; 576–581.

[12]. Hamedheidari S, Rafeh R. A novel agent-based approach to detect sinkhole attacks in wireless sensor networks. *Computers & Security* 2013; **37**(0): 1–14.

[13]. Salehi SA, Razzaque MA, Naraei P, Farrokhtala A. Detection of sinkhole attack in wireless sensor networks. International Conference on Space Science and Communication (IconSpace 2013), Melaka, Malaysia, 2013; 361–365.

[14]. Hamedheidari S, Rafeh R. A novel agent-based approach to detect sinkhole attacks in wireless sensor networks. *Computers & Security* 2013; **37**(0): 1–14.

[15]. Fessant FL, Papadimitriou A, Viana AC, Sengul C, Palomar E. A sinkhole resilient protocol for wireless sensor networks: performance and security analysis. *Computer Communications* 2012; **35**(2): 234–248.

[16]. Dong D, Li M, Liu Y, Li X, Liao X. Topological detection on wormholes in wireless ad hoc and sensor networks. *IEEE/ACM Transactions on Networking* 2011; **19**(6): 1787–1796.

[17]. Wang SS, Yan KQ, Wang SC, Liu CW. An integrated intrusion detection system for cluster-based wireless sensor networks. *Expert Systems with Applications* 2011; **38**(12): 15234–15243.

[18]. Sharma, Gaurav, et al. "Security in wireless sensor networks using frequency hopping." International Journal of Computer Applications 12.6 (2010).

[19]. Chen C, Song M, Hsieh G. Intrusion Detection of Sinkhole Attacks In Large-scale Wireless Sensor Networks. Proceedings of Wireless Communications, Networking and Information Security (WCNIS), IEEE 2010. p. 711-6.

[20]. Hai TH, Huh EN, Jo M. A lightweight intrusion detection framework for wireless sensor networks. *Wireless Communications and Mobile Computing* 2010; **10**(4): 559–572.

[21]. S. Sharma, "Energy-efficient Secure Routing in Wireless Sensor Networks", Dept of Computer Science and Engineering, National Institute of Technology Rourkela, Rourkela, Orissa, 769 008, India, 2009.

[22]. Vu, Tuan Manh, Carey Williamson, and Reihaneh Safavi-Naini. "Simulation modeling of secure wireless sensor networks." Proceedings of the Fourth International ICST Conference on Performance Evaluation Methodologies and Tools. 2009.

[23]. Papadimitriou A, Fessant FL, Viana AC, Sengul C. Cryptographic protocols to fight sinkhole attacks on tree-based routing in Wireless Sensor Networks. *5th Workshop on Secure Network Protocols (NPSec 2009)*, USA, Princeton, 2009; 43–48.

[24]. Krontiris I, Dimitriou T, Giannetsos T, Mpasoukos M. Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks. *Third International Workshop on Algorithmic Aspects of Wireless Sensor Networks (ALGOSENSORS 2007), Lecture Notes in Computer Science*, Springer, Wroclaw, Poland, 2008; 150–161.

[25]. D. Boyle, T. Newe,"Securing Wireless Sensor Networks: Security Architectures", Journal of Networks, 2008, 3 (1).

[26]. X. Du, H. Chen, "Security in Wireless Sensor Networks", IEEE Wireless Communications, 2008.

[27]. J. Granjal, R. Silva, J. Silva, "Security in Wireless Sensor Networks", CISUC UC, 2008.

[28]. Ngai ECH, Liu J, Lyu MR. An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks. *Computer Communications* 2007; **30** (11-12): 2353–2364.

[29]. Du X, Guizani M, Xiao Y, Chen HH. Two tier secure routing protocol for heterogeneous sensor networks. IEEE Transactions on Wireless Communications 2007; 6(9): 3395–3401.

[30]. Ngai, E. C. H., Liu, J. and Lyu, M. R. On the intruder detection for sinkhole attack in Wireless Sensor networks. IEEE communication Society matter expert. Published in IEEE 2006. June. Canada. 3383- 3389.

[31]. da Silva, A.P., Martins, M., Rocha, B., Loureiro, A., Ruiz, L., Wong, H.C.: Decentralized intrusion detection in wireless sensor networks. In: Q2SWinet 2005. Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks, pp. 16–23. ACM Press, New York (2005)

[32]. Onat, I., Miri, A.: An intrusion detection system for wireless sensor networks. In: Proceeding of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, Montreal, Canada, August 2005, vol. 3, pp. 253–259 (2005)

[33]. Y.C. Hu, A. Perrig, D.B. Johnson, Packet leashes: a defense against wormhole attacks, in: Proceedings of INFOCOM '05, March 2005, pp. 1976–1986.

[34]. F. Ye, H. Luo, S. Lu, L. Zhang, Statistical en-route filtering of injected false data in sensor networks, in: Proceedings of INFOCOM '04, March 2004, pp. 2446–2457.

[35]. B. YILMAZ, Y. S. TASPINAR, and M. Koklu, "Classification of Malicious Android Applications Using Naive Bayes and Support Vector Machine Algorithms", Int J Intell Syst Appl Eng, vol. 10, no. 2, pp. 269–274, May 2022.

[36]. Sastry, N., and Wagner, D., 2004. Security considerations for IEEE 802.15.4 networks. In Proceedings of ACM workshop on Wireless security.

[37]. Jones, K., Waada, A., Olaniu, S., Wison, L., and Eltoweissy, M. 2003. Towards a new paradigm for Securing Wireless Sensor Networks. New Security Paradigms workshop 2003.

[38]. Karlof, C., and Wagner, D., 2003. Secure routing in wireless sensor networks: attacks and countermeasures. University of California at Berkeley, USA, Ad Hoc Networks 1 (2003).

[39]. A. D. Wood, J. A. Standovic, and S. H. Son, "JAM: A Jammed-Area Mapping Service for Sensor Networks," in Proc. of the 24th IEEE Real-Time Systems Symposium (RTSS), Dec 2003, pp. 286-297

[40]. Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks," in Proc. of the 22th IEEE INFOCOM 2003, April 2003, pp. 1976-1986.

[41]. Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole detection in wireless ad hoc networks," Department of Computer Science, Rice University, Tech. Rep. TR01-384, June 2002.

[42]. Bisdikian, C. 2001. An overview of the Bluetooth Wireless technology. IEEE Communication Magazine, vol. 39.

[43]. Carman, D., Krus, P., and Matt, B., 2000. Constraints and approaches for distributed sensor network security. Technical Report 00-010, NAI Labs.