International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Detecting Sinkhole and Selective Forwarding Attack in Wireless Sensor Networks

Umashri Karkikatti[1], **Nalini N**[2]

[1]PG Scholar, Computer Science Engineering Department, NitteMeenakshi Institute of Technology, Bangalore-64 India

[2]Professor, Computer Science Engineering Department, Nitte Meenakshi Institute of Technology Bangalore-64, India

Abstract:-*Wireless Sensor Networks (WSN's) are a promising approach that are useful for variety of applications, such as monitoring safety and security of buildings and spaces, military applications, measuring traffic flows, tracking environmental pollutants, etc. Security for WSNs is a very serious and challenging task these days as they have very important personal or national security level information's in them, mainly following are the challenges faced while designing for a robust secure WSNs, the devices in the sensor networks have severe constraints such as minimal energy, minimal computational and communicational capabilities. And secondly, there is an additional risk of physical attacks such as node capture and tampering, eavesdropping etc. Hence we need a technique which can detect the intrusion of any malicious node in the networks, which can create an alarm for taking appropriate steps to secure the information in the WSN. these techniques should be lightweight because of resource-constrained nature of WSNs[1]. As we are aware of the different kinds of attacks for WSNs. In this paper we propose the lightweight robust technique called Received Signal Strength Indicator (RSSI) for detecting Sinkhole attacks in the WSNs. We have built our own protocol and the RSSI techniques are applied to detect the sinkhole attack. The RSSI technique doesn't cause communication overhead because it will not load the ordinary nodes since the presence of EM nodes. Also we propose a lightweight scheme called Traffic Monitor Based Selective Forwarding Attack Detection Scheme. Our approach uses EM nodes to eavesdrop and monitor all traffics of the network.RSSI technique was earlier implemented using visual sense, In this paper we have implemented RSSI technique in NS2 simulator. The simulation results show the efficient detection of the Sinkhole attacks in WSNs.*

Keywords: WSN, RSSI, detecting sinkhole attacks and selective forwarding attack, intruder detection

1. Introduction

Sensor networks will play an essential role in the upcoming age of pervasive computing, as our personal mobile devices will interact with sensor networks in our environment. Many sensor networks have mission critical tasks, so it is clear that security needs to be taken into account at design time.

Sensor networks are always deployed in open and unattended areas, hence they are subjected to adversary, WSNs have limited power supplies, low bandwidth, small memory sizes and limited energy. Above situations require environment to provide security. The resource-starved nature of sensor networks poses great challenges for security. Besides the battlefield applications, security is critical in premise security and surveillance, building monitoring, burglar alarms, and in sensors in critical systems such as airports, hospitals[3].

Most of the sensor network routing protocols are quite simple, and for this reason are sometimes even more susceptible to attacks against general ad-hoc routing protocols. Karlof and Wagner [2] put specific names and methodologies to these attacks. Most network layer attacks are as follows, Spoofed, Altered, or Replayed Routing Information Attack, Selective Forwarding Attack, Sybil Attack, Wormhole Attack, HELLO Flood Attack, Acknowledgement Spoofing Attack, and Sinkhole Attack.

1.1 Security Goals

When dealing with security in WSNs, we mainly focus on the problem of achieving some of all of the following security contributes or services:

- *Confidentiality:* Confidentiality refers to data in transit to be kept secret from eaves droppers. Here symmetric key ciphers preferred for their low power consumption.
- *Integrity:* Integrity measures that the received data is not altered in transit by an adversary.
- *Authentication:* Authentication enables a node to ensure the identity of the peer with which it is communicating.
- *Availability:* The service should be available all the time.
- *Data Freshness:* It suggests that the data is recent, and it ensures that no old messages have been replayed.
- *Non-repudiation:* It denotes that a node can not deny sending a message it has previously sent.
- *Authorization:* It ensures that only authorized nodes can be accessed to network services or resources.

1.2 Attacks on Wireless Sensor Networks

Major attacks on sensor networks are as follows.

- *Jamming:* Jamming interferes with the radio frequencies of the sensor nodes. If the adversary can block the entire network then that constitutes complete DoS.
- *Tampering:* A tampering attacker may damage a sensor node, replace the entire node or part of its hardware to gain access to sensitive information, such as shared cryptographic keys.
- *Spoofed, altered or replayed routing information:* The attacker can complicate the network and create routing loops, attracting or repelling traffic, generating false error messages, partitioning the network.
- *Sybil Attack:* A malicious node which presents multiple identities to the network is called Sybil attack.

- *Wormholes:* The adversary tunnels messages received in one part of the network over a low latency link, to another part of the network where the messages are then replayed.
- *Hello flood attacks:* In many routing protocols, nodes broadcast hello messages to announce their presence to their neighbors. A node receiving such a message can assume that the node that sent the message is with in its range. An attacker with a high-powered antenna can convince every node in the network that it is their neighbor.
- *Sinkhole Attack:* In a sinkhole attack, the adversary's goal is to attract the traffic from a particular area through a compromised node e making it more attractive e to surrounding nodes with respect to the routing algorithm. Creating a large "sphere of influence", attracting all traffic destined for a base station from nodes several hops away from the compromised node.

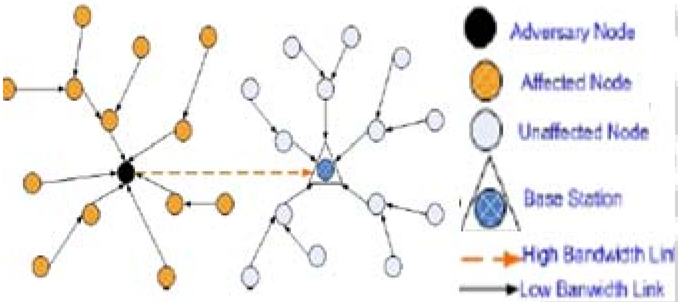


Figure1: Sinkhole Attacks

As in the above figure 1 shows about the sinkhole attack. We can clearly see the black coloured adversary node attracting the traffic from the yellow coloured affected nodes as it advertises for a high quality shortest route to the BS.

Selective forwarding Attack: In a selective forwarding attack [13], malicious nodes behaves like black hole and may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further. A more subtle form of this attack is when an adversary selectively forwards packets. An adversary interested in suppressing or modifying packets originating from a few selected nodes can reliably forward the remaining traffic.

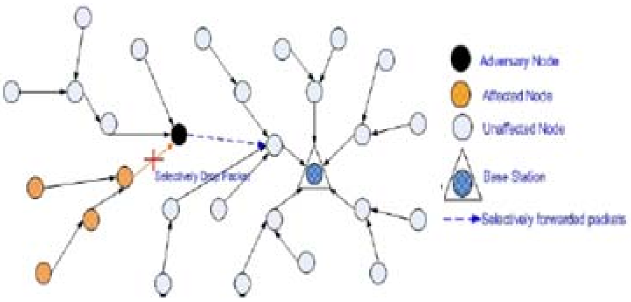


Figure 2: Selective Forwarding Attack

In the above figure 2 shows clearly about Selective Forwarding attack. The selective forwarding attacks are smarter attacks than the Sinkhole attacks. In these attacks, the attacker selectively drops packets based on some predefined criterion, which makes it even harder to detect. Even though there can be many different versions of these attacks, in our implementation, we focus on an address based selective forwarding attack. As shown in Fig. 2, the attacker selectively drops packets based on the source address. In this example, the attacker forwards all packets except from orange nodes.

2. Related Work

The first theory for the detection of sinkhole attack was proposed by Ngai [4]. This approach involved base station in the detection process, wherein it sends the request for all the nodes in the network for their IDs. In return the nodes reply their IDs to the BS. The ID consist of the node position, next hop position and the associated cost. The information received is then used to build a network flow graph for identifying the sinkhole.

Krontiris used a distributed rule based detection system to detect sinkholes [5]. Two rules are implemented in the intrusion detection system. An alarm is sent by the intrusion detection system when either one of the rules is violated by one of the nodes. The two rules are: Rule1:"For each overhead route update packet check the sender field, which must be different than your node ID. If this is not the case, produce an alert and broadcast it to your neighbors."

Rule2:-"For each overhead route update packet check the sender field, which must be the node ID of one of your neighbors. If this is not the case, produce an alert and broadcast it to your neighbors." A collaborative approach can then be used to identify and exclude the sinkhole.

In later work Krontiris, Giannetsos and Dimitriou used a similar rule based approach [6]. Their two rules were: "For each overheard route update packet, check the sender field, which must belong to one of your neighbors" and "For each [parent, child] pair of your neighbors, compare the link quality estimate they advertise for the link between them. Their difference cannot exceed 50." While this approach will not by itself identify the sink hole, extension to a collaborative approach should.

Yu [14] proposed a lightweight security scheme for detecting selective forwarding attacks. The detection scheme uses a multi-hop acknowledgement technique to launch alarms by obtaining responses from intermediate nodes.

3. Assumptions and Network Model

WSNs has many sensor nodes and a BS, sensor nodes are characterized by low power, low bandwidth, low communication and computational capabilities, where as BS has a high bandwidth, high power and hence multiple nodes can send data to BS for processing, it is called as many-to one communication model, which is at a very high risk of sinkhole attack. The intruder with unfaithful routing information attracts the surrounding nodes and then alters the data or perform selective forwarding attack. Most of the current routing protocols in the sensor networks are susceptible to the sinkhole attack.

The physical displacement attack is very harmful for the WSNs because it can lead to start of other more severe attacks. We assume at the beginning a static network, next we assume that attackers can physically displace or remove some of the sensor nodes. Finally we assume that the BS and EM node are physically protected or has temper robust hardware [8], hence it acts as central trusted authority in our algorithm design.

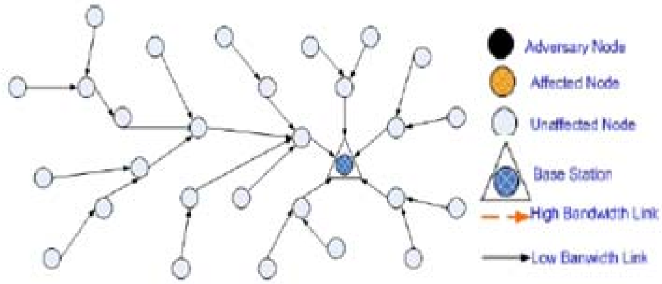


Figure 3: Network Model

4. RSSI Based Technique to Detect Sinkhole Attack

4.1 Calculating the RSSI value

Tumrongwittayapak and Varakulsiripunth proposed a system that uses the RSSI (Received Signal Strength Indicator) value with the help of extra monitor (EM) nodes to detect sinkhole attacks [9 10]. The RSSI [7] techniques used measures the power of the signal at the receiver. The RSSI has been used mainly for RF signal, and the estimate unit is dBm or mW. We assume bidirectional radio links between two neighboring sensors. Referring the path loss based approach model, we calculate the distance between the transmitter and receiver with the effective propagation loss like multi-path propagation and shadow fading. Most widely used signal propagation model [11] is the lognormal shadowing model shown as below,

$$R(d)=P_T - PL(d_0) - 10\eta\log_{10}(d/d_0) + X_\sigma \qquad (1)$$

Where, R (d) is the RSSI value recorded at distance d, PT is the transmit power, PL(d0) is the path loss for a reference distance d0, η is the path loss exponent, and X_σ is a Gaussian random variable with zero mean and σ^2variance, that models the random variation of the RSSI value. RSSI-based localization scheme is introduced in [12].It argues that if at least four sensors monitor radio signals, then no user can hide its location. Suppose node *Emi* receives radio signal from node A, then the RSSI is

$$R_{Emi}=(P_A.K)/(d_{Emi})^\alpha \qquad (2)$$

Where P_A represents transmitter power at node A,R_{EMi}isRSSI value, *K* is constant, $d_{EMi}$is Euclidean distance between node EMiand node A, and α is distance-power gradient. Suppose node j receives radio wave from node A at the same time, then the $R_{EMi}$is similar to equation.

The RSSI ratio of node EMito EMjis

$$R_{Emi}/R_{EMj}=((P_A.K)/(d_{Emi})^\alpha)/((P_A.K)/(d_{Emj})^\alpha) \qquad (3)$$

And the user's location (x, y) can be computed by solving following equation through four receivers EMi, EMj, EMkand EMl:

$$(x-x_{EMi})^2+(y-y_{EMi})^2 = (R_{EMi}/R_{EMj})^{1/\alpha}((x-x_{EMj})^2+(y-y_{EMj})^2)$$
$$(x-x_{EMi})^2+(y-y_{EMi})^2 = (R_{EMi}/R_{EMk})^{1/\alpha}((x-x_{EMk})^2+(y-y_{EMk})^2)(4)$$
$$(x-x_{EMi})^2+(y-y_{EMi})^2 = (R_{EMi}/R_{EMl})^{1/\alpha}((x-x_{EMl})^2+(y-y_{EMl})^2)$$

Where $x_{EMi}$and $y_{EMi}$is the location of node EMi, and other notation is similar.

4.2 Visual Geographic Map Creation

When the network initializes, an assumption is made that an intruder will not attack for at least the first T periods, termed as Safe period, so that the system can learn about the normal behavior of the network such as routing information, position of all sensor nodes. Then we calculate a Visual Geographic Map (VGM) of the network by using RSSI value from the EM nodes. The visual geographic map is the graphical representation of the network model and simulates the traffic flow from the nodes to the BS.

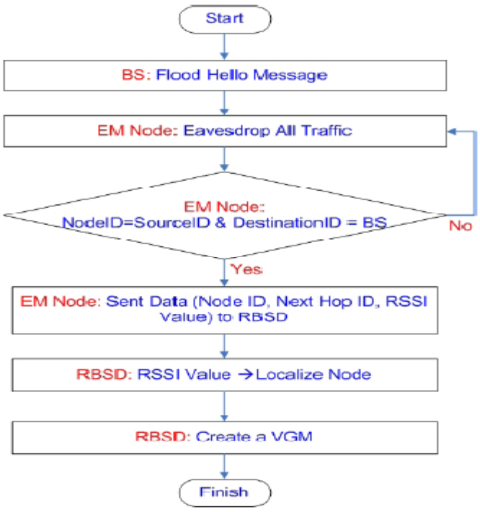


Figure 3: Flowchart of VGM Creation

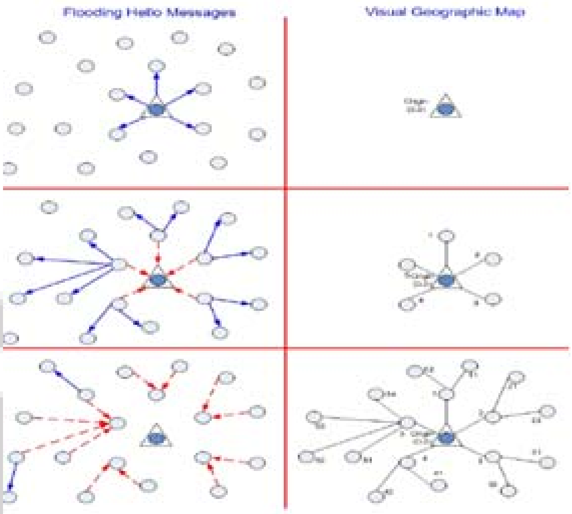


Figure 4: Flowchart of VGM Creation

The BS has one of the four EM nodes and the RSSI Based Sinkhole Detector (RBSD) attached to it. The position of the BS is assumed to be (0,0). The process for VGM creation is as follows, firstly BS floods the Hello message to all sensor nodes in the network and the sensor nodes in return reply answer message to the BS. EM nodes have been monitoring all the traffic in the network. If the destination field of the receive message is BS and Node ID =Source ID, then EM nodes will send data(Node ID, Next hop ID, RSSI value) to RBSD, as shown in fig 4. Finally the RBSD creates the

VGM depending on the data from the four EM nodes as shown in figure 5.

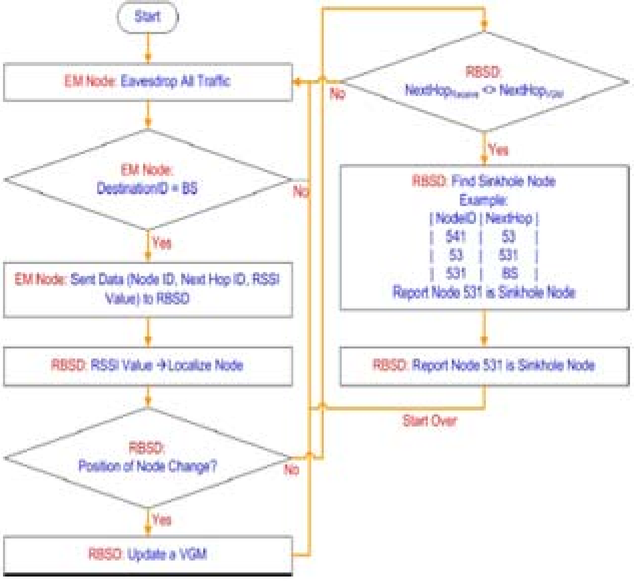


Figure 5: Generating the Visual Geographic Map

4.3 RSSI based sinkhole attacks detection scheme

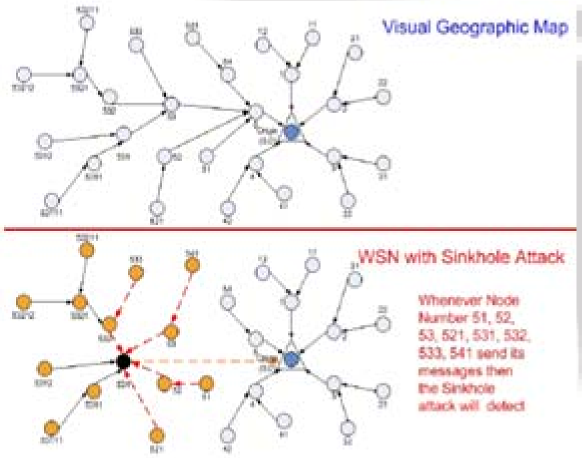


Figure 6: Flowchart of RSSI Based Sinkhole Attacks Detection Scheme

A brief explanation of our scheme is as shown in the figure below. Whenever any sensor node sends its message to the network, all the four EM nodes will receive the message and RSSI value. Next if the destination of the received message is BS, then all of the EM nodes will send RSSI value to RBSD to determine the position of the sensor nodes, then the VGM is updated. If the normal flow of the message is not seen in the VGM, then the Sinkhole attack is detected as shown in the figure6 and 7.

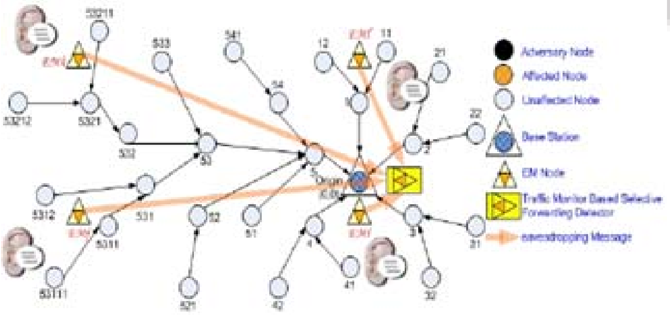


Figure 7: Detecting Sinkhole Attacks

5. Traffic Monitor Based Selective Forwarding Attacks Detection Scheme

The Selective forwarding attack is a byproduct of sinkhole attack; it is much more dangerous than Sinkhole attack. We propose a lightweight scheme called as Traffic Monitor based Selective forwarding attack detection scheme. Our protocol uses EM nodes to monitor all the traffic of the network as shown in the figure below.

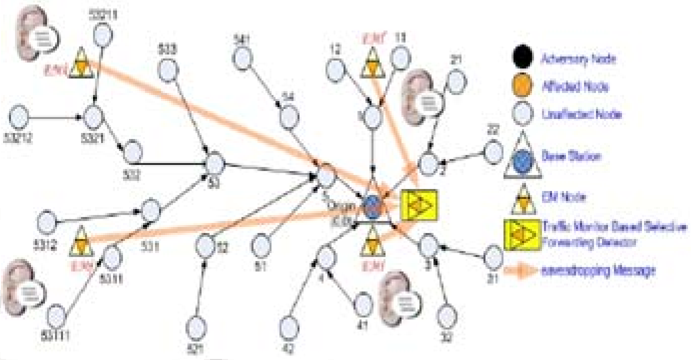


Figure 8: Traffic Monitor Based Selective Forwarding Attacks Detection Scheme

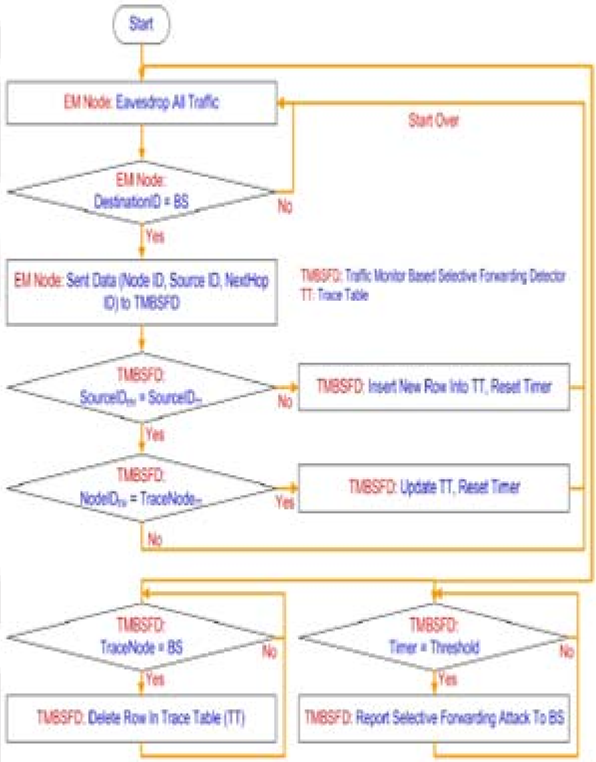
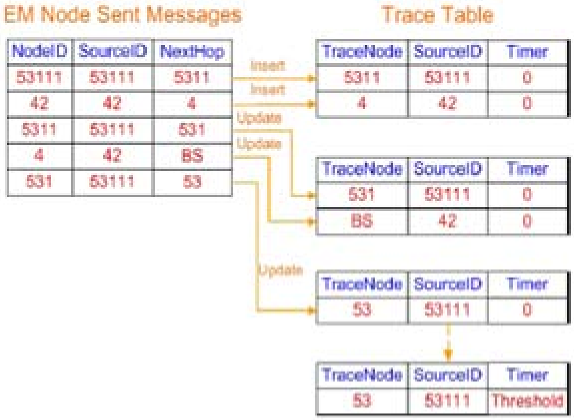


Figure 9: Flowchart of Traffic Monitor Based Selective Forwarding Attacks Detection Scheme

As we see in the above algorithm EM node eavesdrops all the traffic in the network, And if the destination is BS then EM node generates the data (Node ID, Source ID, NextHop ID) to TMBSFD (Traffic Monitor Based Selective Forwarding Attacks Detector).TMBSFD then creates the trace table for the comparison of the data and hence for detecting of the selective forwarding detection. TMBSFD checks first for if Source ID_{EM}=Source ID_{TT} , if this condition is NO then it resets the timer and the process again starts over else it checks for the next condition as Node ID_{EM}=Node ID_{TT} if this condition is YES then it updates the

TT and reset the timer. Later it checks if Trace node = BS then it deletes the entire row in the TT else it checks for the timer threshold value, if it is more than the threshold value then it detects as Selective forwarding attack happening.

Trace table contains 3 columns mainly Trace node, Source ID and Timer. TMBSFD inserts the data in the row for each SourceID$_{EM}$=SourceID$_{TT}$ and updates the same if Node ID$_{EM}$=Node ID$_{TT}$, the third column timer is the time taken for every transaction between the source node and the BS. A threshold value is set and checking is done for the time for every transaction.



EM Node Sent Messages

NodeID	SourceID	NextHop
53111	53111	5311
42	42	4
5311	53111	531
4	42	BS
531	53111	53

Trace Table

TraceNode	SourceID	Timer
5311	53111	0
4	42	0

TraceNode	SourceID	Timer
531	53111	0
BS	42	0

TraceNode	SourceID	Timer
53	53111	0

TraceNode	SourceID	Timer
53	53111	Threshold

Figure 10: Example of EM Message and Trace Table

6. Simulation Setup and Results

We simulate a WSN with 100m X 100mfield in which 25 nodes are placed with uniform random distribution. The sensors have radio range of 40m. A BS is placed at the centre of the network to collect data from the sensors. After that a sinkhole is added to the network at random coordinates of x,y for emulating a sinkhole attack.

Table1: Parameter Settings

Parameter	*Value*
Simulation Area	100mX100m
No of Sensor nodes	25
Transmission Range	40m
Routing Protocol	AODV
Data Rate	20 per 0.005 sec
Packet Size	64bytes
Simulation Time	12sec

We evaluate the performance of our sinkhole detection algorithm through simulations. We have used NS-2 [15] for the simulation wireless sensor networks. Sensor network packages [16]are configured on the top of NS-2, which involves the configuration of phenomenon channel, data channel, phenomenon nodes with phenomenon routing protocol to capture real time events, phenomenon nodes pulse rate, phenomenon type, sensor nodes, non-sensor nodes, sensor agents, UDP agents, sensor applications etc. Fig 11 shows the screen of our simulation.

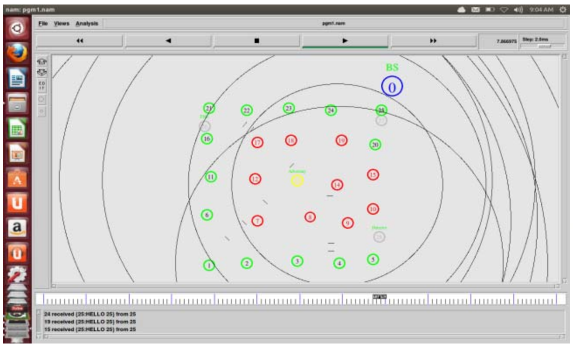


Figure 11: Simulation Screen

The success rate represents the percentage that our algorithm can correctly identify the sinkhole, the false positive rate represents the percentage that our algorithm identifies sinkhole falsely and the false negative rate represents the percentage that our algorithm is not able to identify any sinkhole but it exists. The graph below shows the success rates for dropping rates of 0, 0.2, 0.4, 0.6 and 0.8 respectively. 0 % dropping rates, we see that the success rates are 100%. From 20- 80% dropping rates the success rates are almost near to 100%.

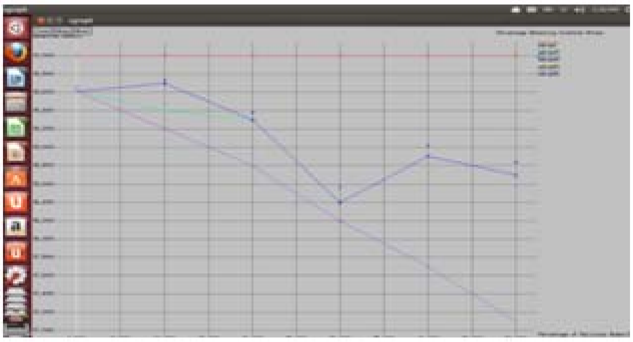


Figure 12: Percentage of detecting Sinkhole Attacks

Figure 13 and Figure 14 shows the false-positive rate and false negative rate in detecting sinkhole attacks. The simulation results indicate that the error rates are quite low. There is no false-positive and false-negative errors when dropping rate is in between 0% to 40%.The error rates increase slightly with increasing of the dropping rate and the number of malicious nodes. When the number of malicious nodes increases, there is more incorrect network flow information provided to the *BS*. If many correct messages are dropped, the remaining wrong information can mislead the *BS*. The *BS* may incorrectly detect the malicious node and lead to a false-positive error. Similarly, the *BS* may receive inadequate number of messages to identify the intruder and bring a false-negative error.

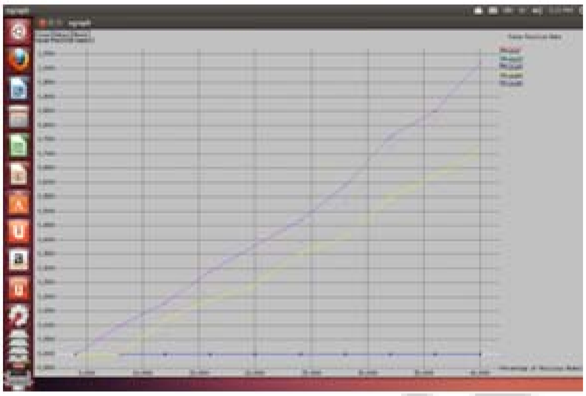


Figure 13: Detecting Sinkhole Attacks: False Positive Rate

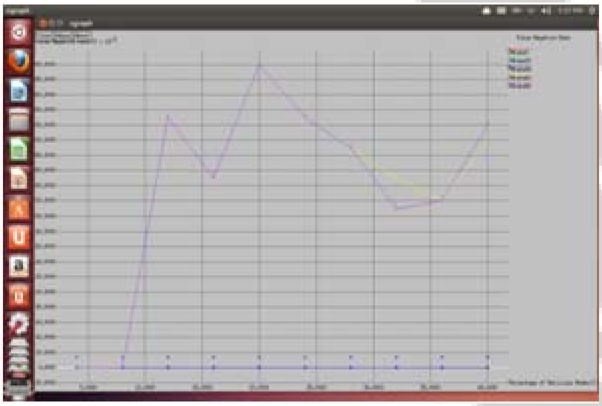


Figure 14: Detecting Sinkhole Attacks: False Negative Rate

The below Figure15 shows Percentage of Detecting Selective forwarding Attacks which Trace Table size equal 128Bytes and Threshold value > 70milliseconds.The results as seen are accurate and hence showcase effective efficient Selective Forwarding Attack Detection. Figure 16 shows the result of False Negative Rate and Figure 17 shows the result of False Positive Rate.

Figure 15: Percentage of Detecting Selective Forwarding Attacks

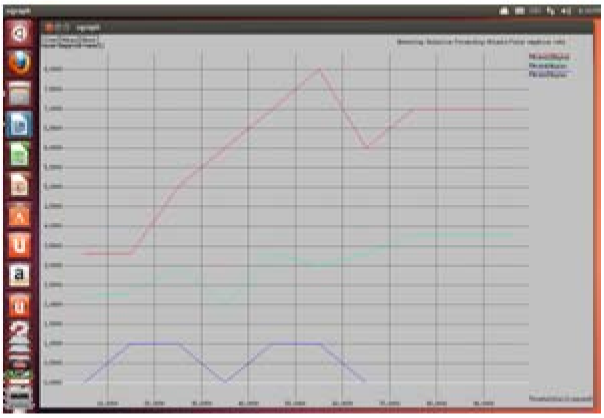


Figure16: Detecting Selective Forwarding Attack- False Negative Rate

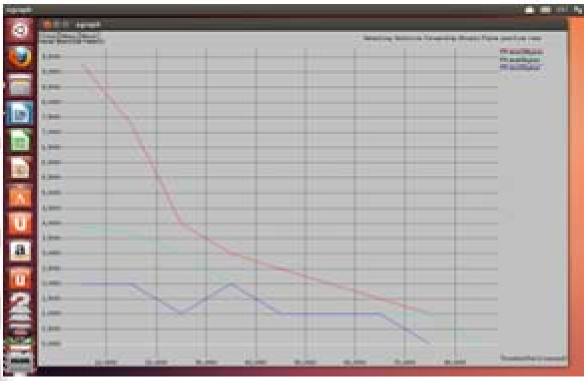


Figure 17: Detecting Selective Forwarding Attack- False Positive Rate

7. Conclusion and Future Scope

In this paper, we presented an effective method for identifying sinkhole attacks in a wireless sensor network. We introduced RSSI-based lightweight solution for detecting the Sinkhole attack in WSN. The functionality of the detection scheme is tested and the performance is analyzed in terms of detection accuracy. Also we proposed a lightweight scheme called Traffic Monitor Based Selective Forwarding Attack Detection Scheme. We have implemented RSSI technique in NS2 simulator. The simulation results show the efficient detection of the Sink hole attacks and Selective Forwarding Attacks in WSNs. We achieved etection with 100%completeness and less percentage of false positive rates. In future work we will try to answer how we can extend our protocol to cope with other attacks in the WSNs.

References

[1] Krontiris, T. Giannetsos, T. Dimitriou, " LIDeA: A Distributed Lightweight Intrusion Detection Architecture for Sensor Networks", SECURECOMM'08: Fourth International Conference on Security and Privacy for Communication Networks, Istanbul, Turkey, September 22- 25, 2008.

[2] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", In First IEEE International Workshop on Sensor Network Protocols and Applications, pages 113–127, May 2003.

[3] M. Saraogi, " Security in Wireless Sensor Networks", Department of Computer Science, University of Tennessee, 2005, unpublished.

[4] E. C. H. Ngai, J. Liu, and M. R. Lyu, “On the intruder detection for sinkhole attack in wireless sensor networks,” in Proceedings of the IEEE International Conference on Communications (ICC ’06), Istanbul, Turkey, June 2006.

[5] Krontiris, T. Dimitriou, T. Giannetsos and M. Mpasoukos, “Intrusion detection of sinkhole attacks in wireless sensor networks”, ALGO SENSORS’07 Proceedings of the 3rd international conference on Algorithmic aspects of wireless sensor networks, (2007).

[6] Krontiris, T. Giannetsos and T. Dimitriou, “Launching a Sinkhole Attack in Wireless Sensor Networks; The Intruder Side”, 2008 IEEE InternationalConference on Wireless and Mobile Computing, Networking and Communications, (2008).

[7] K. Pahlavan, and X. Li, “Indoor Geo-location Science and Technology”, IEEE Communications Magazine, Feb. 2002, Vol. 40, no.2, pp.112-118.

[8] E. Shi, A. Perrig, “Designing secure sensor networks”, IEEE Wireless Communications 11 (2004) 38–43.

[9] C. Tumrongwittayapak and R. Varakulsiripunth, “Detecting Sinkhole attacks in wireless sensor networks”, ICROS-SICE International Joint Conference, **(2009)**, pp. 1966-1971.

[10] C. Tumrongwittayapak and R. Varakulsiripunth, “Detecting sinkhole attack and selective forwarding attack in wireless sensor networks,” 2009 7th International Conference on Information, Communcations and Signal Processing (ICICS), **(2009)**, pp. 1-5.

[11] D. Lymberopoulos, Q.Linsey, and A. Savvides, “ An Empirical Characterization of Radio Signal Strength Variability in 3-D IEEE 802.15.4 Networks using Monopole Antennas”, In Proceedings of Third European Workshop on Wireless Sensor Networks, Springer Berlin, Heidelberg, Jan. 2006, pp.326-341.

[12] S. Zhong, L. Li, Y. G. Liu, and Y. R. Yang, “Privacy-preserving location based services for mobile users in wireless networks.” Technical Report YALEU/DCS/TR-1297, Yale Computer Science, July 2004.

[13] Wang Xin-sheng, Zhan Yong-zhao, XiongShu-ming, and Wang Liangmin. Lightweight defense scheme against selective forwarding attacks in wireless sensor networks. pages 226 –232, oct. 2009.

[14] Bo Yu, Bin Xiao, " Detecting Selective Forwarding Attacks in WirelessSensor Networks", In the proceedings of Parallel and Distributed Processing Symposium, 2006.

[15] “Network Simulators”, [Online] Available: http://www.isi.edu/nsnam/ns/

[16] “Simulating Sensor Networks in NS-2”,[Online] Available:http://nile.wpi.edu/NS/

Author Profile

Dr. Nalini N is currently working as Professor in computer science engineering in Nitte Meenakshi Institute of Technology Bangalore-64

Umashri Karkikatti is currently pursuing masters degree program in computer science engineering in Nitte Meenakshi Institute of Technology Bangalore-64 India.