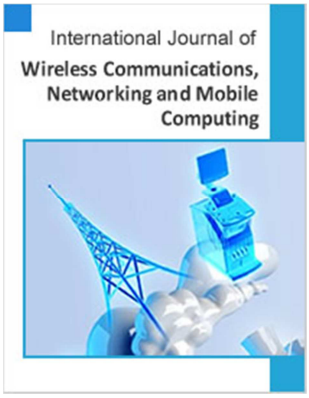
International Journal of Wireless Communications, Networking and Mobile Computing
2016; 3(5): 48-52
http://www.aascit.org/journal/wcnmc
ISSN: 2381-1137 (Print); ISSN: 2381-1145 (Online)

American Association for Science and Technology



Keywords
Blackhole,
Malicious,
AODV,
SVM,
Contigency

Received: April 29, 2016
Accepted: May 9, 2016
Published: September 26, 2016

Blackhole Attack Detection in Wireless Sensor Networks Using Support Vector Machine

Mehndi Samra, Naveen Kumar Gondhi

School of Computer Science Engineering, Shri Mata Vaishno Devi University, Katra, India

Email address
mehndi.samra16@gmail.com (M. Samra), naveen.gondhi@smvdu.ac.in (N. K. Gondhi)

Citation
Mehndi Samra, Naveen Kumar Gondhi. Blackhole Attack Detection in Wireless Sensor Networks Using Support Vector Machine. *International Journal of Wireless Communications, Networking and Mobile Computing.* Vol. 3, No. 5, 2016, pp. 48-52.

Abstract
The paper demonstrates simulation of blackhole attack in wireless sensor networks. A node is considered suspicious in case there is a large drop of packets by the node and as a result very little or none of the packets are able to reach the destination. The paper proposes first a modified AODV routing protocol for simulating a blackhole second detecting the same using contingency table generated by the model based on support vector machine.

1. Introduction

A wireless sensor network (WSN) is a mesh network consisting of a set of compact and automated devices. These devices are known as sensing nodes having its own resources and computational capability. These nodes are distributed across a well-defined area representing an ad hoc network and are able to communicate among themselves. In a wireless sensor network there is a class of certain special nodes with the capacity to process and store the information collected over the network. These nodes are better known as sink nodes. The communication between two nodes is over multiple hops if they are not within each other's transmitting and receiving range [1].

Wireless sensor network are used to gather essential data from the installed environment where they are embedded. The data collected is processed by the sensor nodes and then forwarded over non-secure channels to sink node for further processing. The sensor networks have vast application in the areas of environment, infrastructure, public safety, medical, security and transportation.

These applications areas are open and likely to be attacked. Many different types of attacks known to exist in a WSN including spoofing the various fields of a message packet while it is in transit. It is done in such a way that the recipient receives is an altered copy instead of original message being sent by the source [2].

A well-known denial of service attack in which a malicious node attracts all packets by false claiming a new route to the destination. It absorbs all the packets without forwarding them to the destination.

A black hole node is actually the one that always respond to every RREQ message with a RREP message. Even when it does not have an actual route to the destination node. When the data packet reaches the black hole node. It drops all the packets instead of forwarding them to next in route hop. As a result none of the packets are able to reach the destination.

The packet dropping attack as described as black hole node attack is demonstrated in the paper. In which a malicious node absorbs all the data packet and is similar to the

black hole in the universe which absorbs everything that comes to it. It makes use of all the liabilities towards the route discovery packets of the on demand protocol better known as AODV [3].

In fact the blackhole attack in wireless sensor network makes to compromise route establishment in a network. A malicious node that broadcasts a routing message with an extra ordinary high power is able to mislead a large number of nodes. These nodes attempt to use the malicious node as their next hop in their route to the sink. But the nodes those are at a far-away distance would simply be sending their messages in the state of unawareness. A similar scenario, blackhole attack acting as a malicious node is able to convince all neighbouring nodes those are normally multiple hops from the sink node that they are actually one hop away from the destination node. These nodes in response try to send their packets directly to the sink node, which is unable to hear them [4].

Hu, Perrig, and Johnson have presented a novel approach to countermeasure these malicious attacks in ad hoc networks. It includes additional information to be encapsulated to the standard packets in order to restrict its maximum allowed travel distance. The mentioned approach is known as packet leash. The packet leash approach has its own disadvantages including the increase in the processing time of the packets and in its size [5].

The research involves a mechanism based on analyzing the behaviour characteristics of each node present in the wireless sensor network during transmission. The simulation was performed against two cases one in the presence of malicious node which acts as a blackhole and the second, when the said node behaved as non-malicious or in other words in the absence of blackhole attack. The separate trace files are generated by monitoring the network behavior during transmission. The analysis of generated trace files in said cases is carried out using support vector machine based model leading to the prediction of a suspected node as a blackhole.

The features including total packets send, received, forwarded and dropped at each hop were monitored, recorded and provided as an input to the classification model.

2. Simulation Model

In the paper a homogenous WSN is considered. Which consist of network nodes having similar hardware and software configuration. The simulating environment is assumed to possess symmetricity in which node can only communicate with another node if and only if Y can communicate with X. All the nodes in the network are having the same operating characteristics. Which includes transmission power (Tx), antenna height (h) and antenna gain (g) throughout the lifetime of the network. All nodes are having unique identification and fixed geographical position. The geographical position of each node can be obtained using a GPS positioning system. The value of a geographical position of each node as well as its identifier is encapsulated in each of the messages it sends. It is also assumed that message exchanges in the network are encrypted in order to provide necessary security in the network. The radio propagation is further assumed to follow a well-defined model, which includes the Free Space Model and the Two- Ray Ground Model [6]. They specify how the values of transmission power, received signal strength and distance between the transmitter and the receiver relate to each other.

In this paper a wireless sensor network is considered to satisfy following axioms:

(1) Homogenity[1] In which all nodes in the network are having same configuration.
(2) Static[2] All the nodes in the network are having predefined fixed coordinates and they do not change their position once deployed.
(3) Symmetricity[3] The simulating environment is assumed to be symmetric in which the node X can only communicate with node Y, in case Y is also able to communicate with X.

Finally, it is assumed that malicious nodes are capable of performing blackhole attack only. The presence of a malicious node is confirmed in case there is large difference in the number of packets sent by the source and the packets received by the predefined destination node. Under mentioned conditions a message, a node can be classified as suspicious or unsuspicious.

This section provides the information regarding simulating environment and results generated. The NS2 is used to simulate the wireless sensor network environment in order to evaluate the data and carry out necessary analysis. The network is created with the properties as mentioned in the table (1) where the channel or the medium for transmission is wireless, the propagation is set to be Two ray ground making an assumption that a signal sent from one node to another does not travel in a straight line or a unique path but eventually also through a reflection in the ground, topology used is wireless physical. The address associated with each node is of type MAC following IEEE standard 802.11. The Improvement of performance at the destination node by applying different types of queues at the routers observed. The droptail queue with priority is implemented where drop of packets can only take place at the rare end of the queue. The congestion and the packet drops can be reduced at the link node by appropriate selection of queue type at the link node [7].

Table 1. *Shows the wireless sensor network configuration.*

S. No.	Attributes	Value
1	Channel	Wireless Channel
2	Propagation	Two Ray Ground
3	Phy	Wireless Phy
4	Mac	802_11
5	Queue	DropTail/PriQueue
6	Link Layer type	LL
7	Antenna	OmniAntenna
8	ifqlen	50
9	Nodes	7
10	Routing protocol	AODV

All the nodes are located on a grid of 900 X 600 field with well-defined specific x and y coordinates. The nodes are located such that no two nodes share the same coordinates on the grid as shown in fig. 1

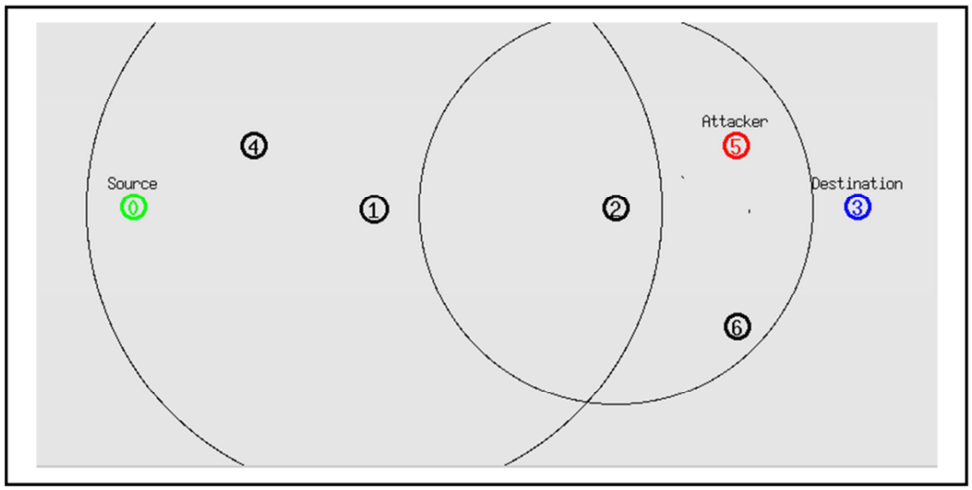


Fig. 1. *Showing the deployment of seven nodes in the wireless sensor network.*

The N number of nodes were used in the simulation. Where N = {n0, n1, n2, n3, n4, n5, n6}. The node n0 is defined as source node, the node n5 as malicious blackhole attack node and node n3 is defined as destination node also known as sink node. The traffic is sent by the source node n0 to the sink node n3 over multiple hops in the network.

3. Simulation Results

The simulation was run for 100 ms with packet size = 1000, traffic type = CBR, traffic rate =0.1Mbs. The AODV routing protocol after making necessary modification is used to perform the desired routing of packets from source to sink node and following observations were made.

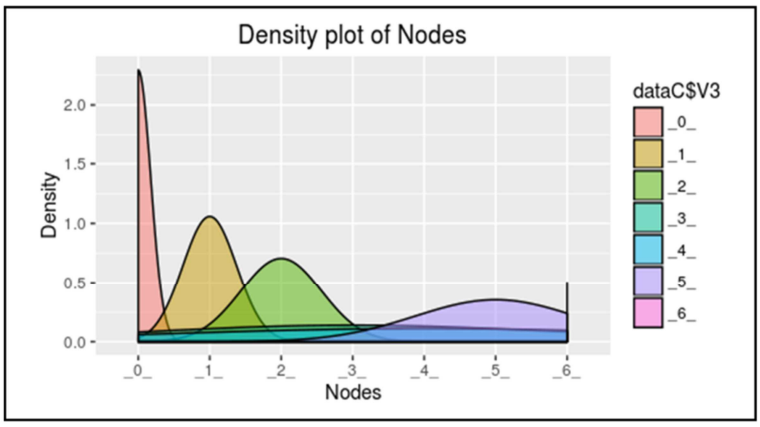


Fig. 2. *Showing the density plot of nodes in presence of blackhole attack.*

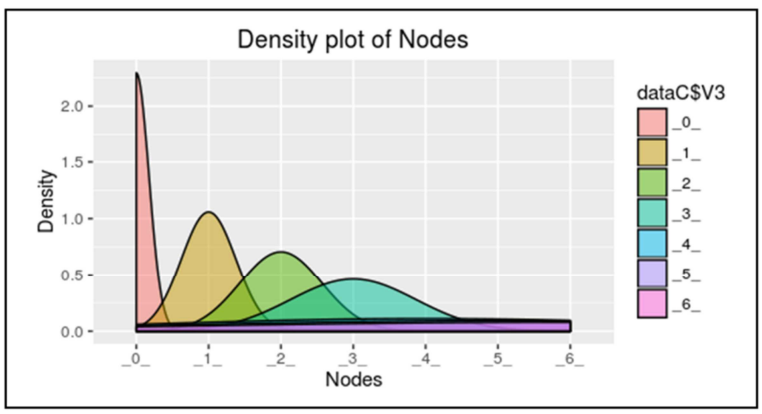


Fig. 3. *Showing the density plot of nodes in absence of blackhole attack.*

Table 2. *Showing total packets send, received, forwarded, dropped and packet density ratio during different intervals in the presence of blackhole attack.*

S. no	Run time	Send	Received	Forwarded	Dropped	Packet density ratio
1	0-10	113	452	228	113	901.769
2	10-20	238	952	478	238	428.151
3	20-30	363	1452	728	363	280.716
4	30-40	488	1952	978	488	208.811
5	40-50	613	2452	1228	613	166.231
6	50-60	738	2952	1478	738	138.075
7	60-70	863	3452	1728	863	118.076
8	70-80	988	3952	1978	988	103.137
9	80-90	1113	4452	2228	1113	91.554
10	90-100	1238	4952	2478	1238	82.310

The increase in the drop of packets was observed in the presence of blackhole attack while the simulation was run over period of 100ms. The number of packets dropped were found to be equal to the number of packets being sent by the source node as shown in table (2).

Table 3. *Showing total packets send, received, forwarded, dropped and packet density ratio during different intervals in the absence of blackhole attack.*

S. no	Run time	Send	Received	Forwarded	Dropped	Packet density ratio
1	0-10	113	339	228	0	901.769
2	10-20	238	714	478	0	428.151
3	20-30	363	1089	728	0	280.716
4	30-40	488	1464	978	0	208.811
5	40-50	613	1839	1228	0	166.231
6	50-60	738	2214	1478	0	138.075
7	60-70	863	2589	1728	0	118.076
8	70-80	988	2964	1978	0	103.137
9	80-90	1113	3339	2228	0	91.554
10	90-100	1238	3714	2478	0	82.310

There was no drop of packets observed in the absence of blackhole attack while the simulation was again run over period of 100ms. The number of packets sent from the source were found to be equal to the number of packets received at the destination as shown in table (3).

The predicted contingency table in the presence of blackhole attack by the SVM model is shown in table (4). It is observed that the total number of packets sent by the source node (n0) = 1238, the number of packets received by the sink node (n3) = 0 as there is drop of 1238 packets at the blackhole node (n5).

Table 4. *Showing the packets dropped, forwarded, received; send as per the contingency table in presence of blackhole attack.*

S. No.	Nodes	D	F	R	S
1	_0_	0	2	1256	1238
2	_1_	0	1238	1857	0
3	_2_	0	0	1857	0
4	_3_	0	0	0	0
5	_4_	0	0	0	0
6	_5_	1238	0	0	0
7	_6_	0	0	0	0

The predicted contingency table was generated without blackhole attack by the SVM model as shown in table (5). It is observed that the total number of packets sent by the source node (n0) = 1238, the number of packets received by the sink node (n3) =1238 as there was no drop in packets in the absence of blackhole attack.

Table 5. *Contigency table showing the packets dropped, forwarded, received; send in absence of blackhole attack.*

S. No.	Nodes	F	R	S
1	_0_	2	1258	1238
2	_1_	1238	1238	0
3	_2_	1238	1238	0
4	_3_	0	1238	0
5	_4_	0	0	0
6	_5_	0	0	0
7	_6_	0	0	0

4. Conclusion

1. It is observed that there is a drop in the density curve with respect to time once the packets travel from source (n0) to sink node (n3) as shown in fig. (2). This drop in the density curve clearly depicts the presence of some malicious activity during the transmission. The low peaks in the density curve for node (n3), (n4), (n5) and (n6) proves these nodes are malicious or not present in the route path.
2. It is observed that there is a no drop in the density curve with respect to time once the packets travel from source (n0) to sink node (n3) as shown in fig. (3). This drop in the density curve clearly depicts the absence of any malicious activity during the transmission.

3. The SVM model was able to predict the malicious node (n5) from the suspected nodes n3, n4, n6 with great accuracy.

References

[1] Berkeley MICA mote. http://webs.cs.berkeley.edu/tos/hardware/hardware.html, 2003.

[2] J. M. Kahn, R. H. Katz, and K. S. J. Pister. Next century challenges: Mobile networking for "smart dust". In *International Conference on Mobile Computing and Networking (MOBICOM)*, pages 271–278, 1999.

[3] Abderrahmane Baadache, Ali Belmehdi "Avoiding-Black-Hole-and-Cooperative-Black-Hole-Attacks-in-Wireless-Ad-hoc-Networks" IJCSIS) International journal of Computer Science and Information Secrity, Vol. 7, No. 1, 2010.

[4] J. M. Kahn, R. H. Katz, and K. S. J. Pister. Emerging challenges: Mobile networking for "smart dust". *Journal of Communications and Networks*, 2 (3): 188–196, September 2000.

[5] Y.-C. Hu, A. Perrig, and D. B. Johnson. Packet leashes: A defense against wormhole attacks in wireless ad hoc networks. *Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003)*, April 2003.

[6] T. S. Rappaport. *Wireless communications: principles and practice*. Prentice Hall, 2nd edition, 2002.

[7] R. Bahl, R. Kumar and J. P. Singh, "Comparison of buffering in Manhattan Street Network in NS2," Communication Systems, Networks and Applications (ICCSNA), 2010 Second International Conference on, Hong Kong, 2010, pp. 441-443.