Indian Journal of Science and Technology, Vol 10(24), DOI: 10.17485/ijst/2017/v10i24/111413, June 2017
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Sinkhole Attack Detection in WSN using Pure MD5 Algorithm

S. Vidhya[1,2]* and T. Sasilatha[3]

[1]Faculty of Computer Science and Engineering, Sathyabama University, Chennai – 600119, Tamil Nadu, India; vidhyas_1983@yahoo.com
[2]Department of Information Technology, Saveetha Engineering College, Chennai – 602105, Tamil Nadu, India
[3]AMET University, Chennai – 603112, Tamil Nadu, India; sasi_saha@yahoo.com

Abstract

Objective: To detect the sinkhole attack in AODV routing in wireless sensor network and provides the security. **Methods**: This employs an energy power consumption mechanism in AODV routing with external energy supplied through the battery. Security is achieved through pure MD5 algorithm detects sinkhole attack and prevents the network from severe attack. This approach provides better performance compared with normal AODV routing. The energy power consumption AODV routing selects the node in the network based on the node which is having more energy to transmit, as a neighbour. This implies that the network continues routing even though any one node in routing possesses less energy to transmit. **Findings/Result:** Simulation result obtained through Ns2 shows that the detection of sinkhole attack using MD5 security algorithm achieves 93% packet delivery rate, 80% throughput and 500 ms end to end delay in the network.

Keywords: Detection, Energy, Intrusion, Sinkhole, Security

1. Introduction

Wireless sensor network consists of small, low cost, low power sensor nodes deployed and distributed over a large geographical area. WSN is deployed in different application areas. Nature makes the sensor network ideally suitable for military, healthcare, industrial and automation areas[1]. Sensor nodes are capable of sensing and monitoring the environment. The collected information is sent to the base station. It is prone to severe attack. Security is a major concern in WSNs. Most of the real world applications do not consider the security aspects.

The study[2] clearly explains the concept of security in different scenarios. Sensor nodes communicate with each other through different routing methods. Sensor network creates an opportunity for attackers to attract the sensor nodes for collecting the information which is communicated. Different types of attacks are present in WSN of which sinkhole attack is one where the malicious node attracts the node around the sink. The adversary node attracts traffic pattern and misroutes the neighbour. It provides fake routing information to the neighbours. So the base station is unable to avail sending and receipt of the entire sensing of data from nodes.

Different types of research methods attempt at providing security mechanisms for overcoming sinkhole attack. The proposed approach provides a solution to meet sinkhole attack. It aims at detecting sinkhole attack and provides the security to the sinkhole attack through security algorithm.

1.1 Security

Security is an important concept to be considered for the network which is deployed in hostile environment. Deployment of a network in a human uninterruptible place is very critical task without security. Design of a security protocol is a challenging task due to the nature and availability of resources. Security mechanisms used for networks can vary accordingly from fixed to wireless networks.

*Author for correspondence

1.2 Sinkhole Attack

Sinkhole attack is a kind of attack where an intruder compromises a node in a network. Figure 1 shows the sinkhole attack in WSN. The compromise node attacks the neighbour nodes on the basis of the information received from the protocol used as routing. The nature of sensor network makes leads to a severe attack due to the compromised nodes near the sink. The source is unable able to send data packets to the sink. This leads to misrouting of data packets.

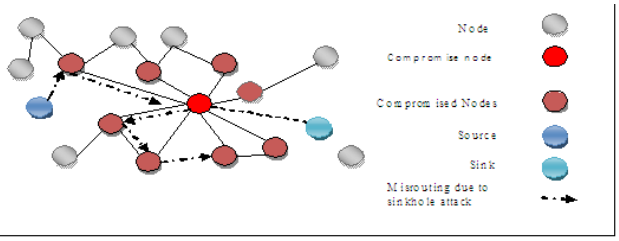

Figure 1. Sinkhole in AODV.

Section 1 presents different types of techniques proposed to detect sinkhole attack and solutions applied for meeting the sinkhole attack. Section 2 discusses about the sinkhole attack. Section 3 discusses the algorithm for the detection of sinkhole attacks and provides a solution. Section 4 describes the simulation results and QOS parameters.

In[3] have proposed a mechanism to prevent and detect sink whole attack in WSN. The approach uses mobile agents along with a trusted node combination listening to the traffic pattern and not to listen to the pattern produced by a malicious node. The simulation results are evaluated for preventing the approach.

In[4] have proposed a low energy adaptive clustering hierarchy protocol with an intrusion detection system for detecting an intruder in the network. Based on the packet transmitted and received in the network, the agent measures the intrusion detection. In the event of an abnormal in the ratio, malicious activity measured. IDS agent alerts the system and stops the malicious activity.

In[5] have proposed a novel method for detecting sinkhole attack in a wireless sensor network based on the redundancy mechanism. Messages are sent to the nodes which actively participated in routing. Based on the reply from nodes, suspicious nodes are identified and malicious nature is confirmed.

In[6] have discussed an approach for detecting a sinkhole attack in a wireless sensor network. Centralized approach is used for detecting regions in the network using geostatistical hazard model. Distributed monitoring approach is used for monitoring neighbours in the network to detect malicious nodes.

In[7] have proposed an agent based behavioural model for detecting intruders in the network. This approach is a risk based approach based on risk factor. They minimized data losses and time to recovery. Agent packet overheads minimized. They used loosely coupled routing protocols.

2. Proposed Approach

The novel design of the work proposes by this author lies in designing of Energy power consumption model in AODV routing protocol. It aims to detect the intruder in the network. Energy power consumption mechanism finds the energy consumption of each every node in the sensor network. The remaining energy in the network nodes try participates in the routing process on the basis of the energy consumption. Whenever the energy of a node get reduced the energy power consumption mechanism supplies external energy through a battery. This maintains the energy in the network. In the approach proposes by the author, it detects the intruder which compromises a node and protects the network against sinkhole attack.

2.1 Network Deployment

The sensor nodes are deployed in an environment to monitor the area in and around the network and collect the sensed information from the sensor nodes and pass it to the sink. In our proposed approach sensor nodes are distribute normally. The source node is meant for sending the data packets and one sink node to receive the data packets form the source. The mobile agents are normal nodes for collecting the information from their neighbours when there is a different behaviour. The collected information is maintained by a trust manager who regularly collects the updated information from mobile agents.

2.2 Mobile Agent

A Mobile Agent is a software code which travels from host to host and performs the task for the user. Mobile agents are deployed mainly for providing communication among the nodes, to support coordination and cooperation in the sensor nodes. In the approach proposes by

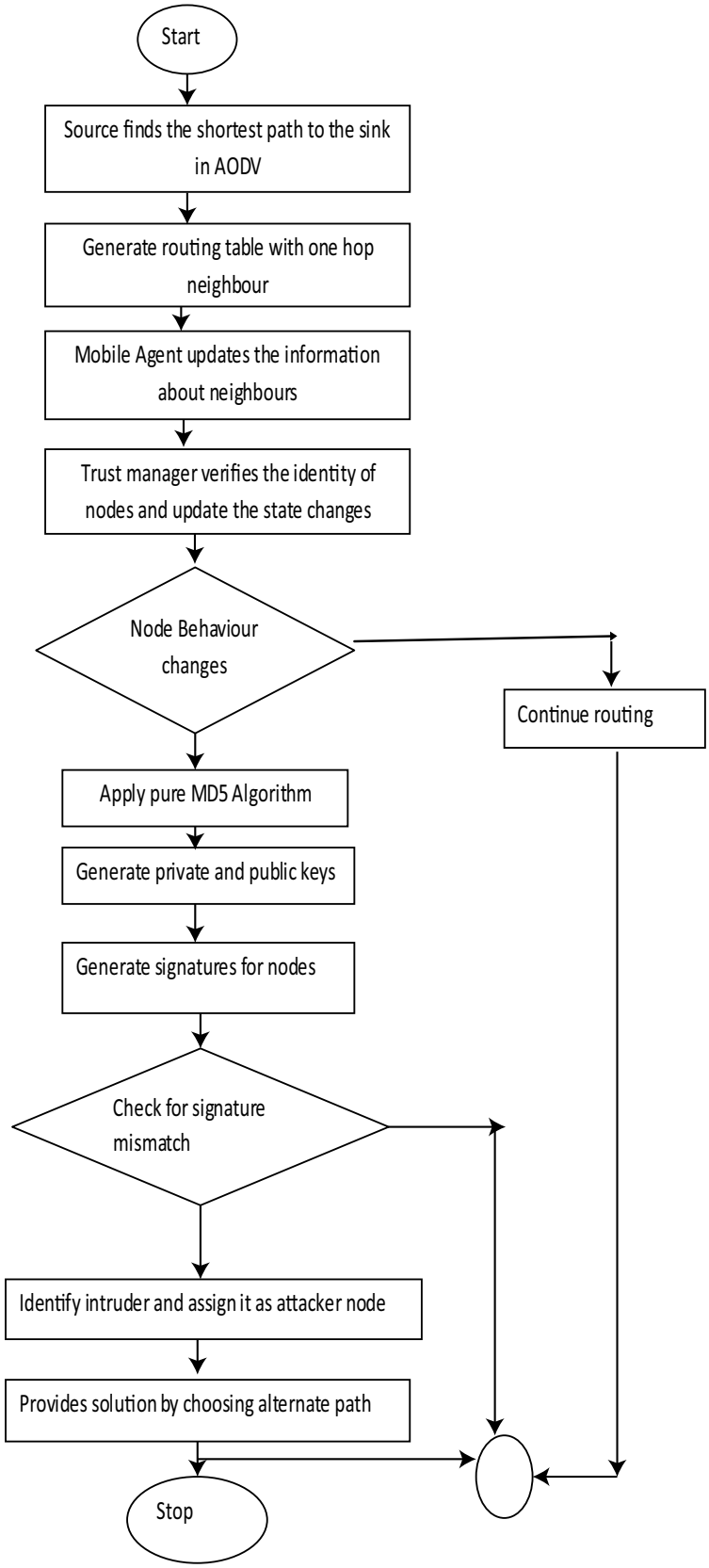

Figure 2. Intrusion detection mechanism for sinkhole attack using MD5 algorithm.

author, mobile agents are used for reducing the communication cost.

2.3 Trust Manager

In the proposed approach the trust manager maintains the entire information in all the nodes in the sensor network. It registers the nodes and verifies their identity. It is supposed to monitor the behaviour of all the nodes in the network. As any change in their behaviour, it is reported to the neighbours in the network. The malicious behaviour is taken it to account to alert the system from severe attack.

2.4 Pure MD5 Algorithm

MD5 algorithm is used in the proposed approach to as a cryptographic with 1-128bit hash function. It has five steps for generating the public key for each node in the sensor network for authentication.

2.5 Intrusion Detection Mechanism

The source finds the shortest path to the sink through AODV routing. In the proposed method, energy power consumption based AODV routing continues the routing considered normal. The novel design selects the nodes with the maximum energy for transmission of it as a neighbour node. The energy of the node gets drained after the completion of the routing process. The nodes with minimum energy cannot continue routing process. Energy power consumption mechanism chooses an alternative path to the destination and supplies external energy through battery. In routing process attacker node tries to attack the nodes present in the sensor network. They introduce fake routing information on the traffic pattern, providing information that about the shortest path to the destination. The neighbour nodes to the attacker node send data packets to the attacker node. Then packets drops occur at the attacker node instead the normal routing. The proposed approach is shown through the following Figure 2.

The Mobile agent updates the change in the state of the node in the network. Periodical information is sent to all the nodes in the network. The Trust manager updates all the system changes and alerts the network of a severe threat. The proposed algorithm proposed by the author pure MD5 generates the public and the private keys. Each node is assigned with a signature. If any attacker node uses the same signature, it is used by a normal node signature that is detected by the proposed algorithm. The Algorithm finds the shortest alternate path to sink and provides the security.

3. Simulation

The proposed approach is evaluated through simulations. NS2 is the simulator used in the author's proposed sinkhole attack using energy efficiency approach using pure MD5 algorithm. Sensor network is randomly deployed with simulation landscape 1500x1500, with 50 sensor nodes. The transmission range is 250m which is the radius of the radio signal. The MAC protocol used in the approach is 802.11. The simulation set up is designed with a 4 sinkhole attacker nodes,3 mobile agents and trust manager. The Received Signal Strength maintains signal loss and reduces the delay in the signal. Table 1 shows the simulation parameters.

Table 1. Simulation parameters.

Parameter	**VALUE**
Simulator	Ns2 - 2.34
Number of Nodes	50
Simulation Time	15 min
Packet Interval	0.01 sec
Simulation Landscape	1500 x 1500
Background Data Traffic	CBR
Size of Data Packet	1000 bytes
Queue Length	50
Transmission Range	100 Kbytes
Node Transmission Range	250 m
Antenna Type	Omni directional
Mobility Models	Random-waypoint (0-30 m/s)
Radio Frequency	850-950 MHz
Routing Protocol	EPC -AODV
MAC Protocol	IEEE 802.11
Parameter	VALUE
Simulator	Ns2 - 2.34
Number of Nodes	50
Simulation Time	15 min
Packet Interval	0.01 sec
Simulation Landscape	1500 x 1500
Background Data Traffic	CBR

Size of Data Packet	1000 bytes
Queue Length	50
Transmission Range	100 Kbytes
Node Transmission Range	250 m
Antenna Type	Omni directional
Mobility Models	Random-waypoint (0-30 m/s)
Radio Frequency	850-950 MHz
Routing Protocol	EPC -AODV
MAC Protocol	IEEE 802.11

4. Results and Discussion

4.1 Packet Delivery Ratio in the Network

Packet delivery rate shown in Figure 3 is defined as the number of data packets delivered in the network in unit time. The detection mechanism proposed by the author has the packet delivery at high 93 % when the nodes in the network number are 50and the curve slowly get reduces to 90 % with 250nodes. It shows that packet rate is high when the node in the network is small in number. Again the curve get reduced to a point to packet ratio is 85 % for 500 nodes in the network. The curve reaches 82 % for 750 nodes in the network. When increase in the nodes from 750 to 1000 is attempted, there is some reduction in the packet delivery ratio to 79% .The overall packet delivery ratio is comparatively high with the approach showing 79%.

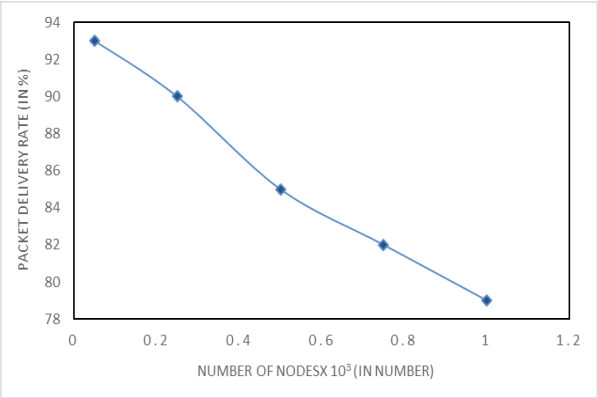

Figure 3. Packet delivery rate in network.

4.2 Throughput in Network

Throughput in the network from Figure 4 shows the efficiency of the proposed approach. The throughput curve shows that the proposed approach reaches 90% in achieving the performance improvement. Initially when the number of nodes in the network is 50, throughput of the network reaches 63 % and there is a slight improvement in throughput when the nodes increase in number from 50 to 250.Again the throughput increases from 67% to 71 % of the throughput value for network with nodes 500. When attempt is made to increase the network size from 500 to 750, throughput of the network goes up from 71% to 76 %. It showing the performance of the author's network. Throughput curve shows an increase from 76% to 83 % for network with a node size 1000.

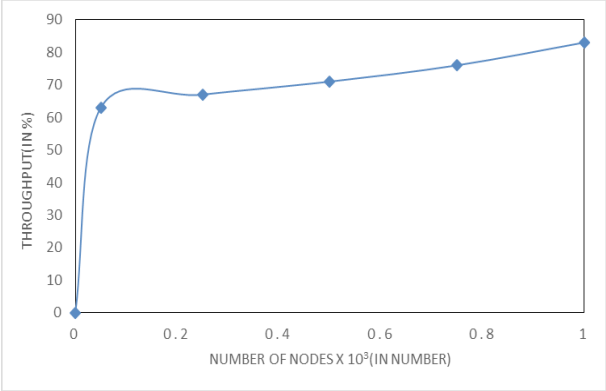

Figure 4. Throughput in the network.

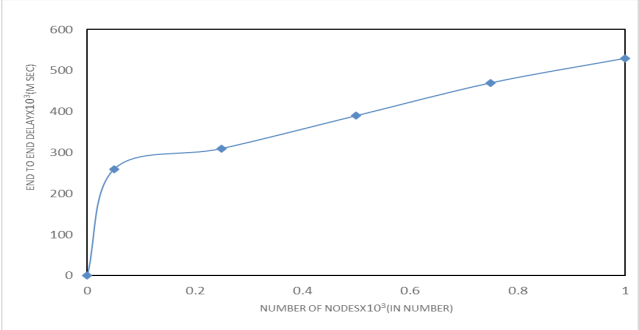

Figure 5. End to end delay in network.

4.3 End to End Delay in Network

The end to end delay in the proposed approach is shown in Figure 5. End to end delay is minimum 0.26 msec when the network contains 50 nodes the curve reaches from 0 to 250. The end to end delay increased progressively reaching 0.31msec for the network with 500 nodes. Again the curve reaches 0.39 msec of the end to end delay for the network with 750 nodes. The curve reaches 0.53 msec end to end delays for the network with 1000 nodes. The end to end delay shows that for a minimum number of nodes in

the network, delay is minimum and the nodes are more with a slight increase of end to end delay in network. This implies some delay in finding the intruder and provides the solution.

5. Conclusion and Future work

The approach proposed by the authors is designed to focus on the security of sensor network. Sensor networks are deployed in areas. Providing security as a tedious work. Researchers are working on many security mechanisms for detecting and recovery of different types of attacks. Two approaches are used in the proposed mechanism. Energy power consumption AODV routing along with external energy mechanism allow sensor networks to continue the routing process with a high degree of efficiency. Intrusion Detection System finds the sinkhole attack and provides a solution through MD5 algorithm. The simulation results show the achievement of throughput for proposed approach.

6. References

1. Sharma K, Ghose MK. Wireless sensor networks an overview on its security threats. IJCA. Mobile Ad-Hoc Networks. 2010; 1:42–5.
2. Perrig A, Stankovic J, Wagner D. Security in wireless sensor networks. Communications of the ACM. 2004; 47(6):53–7. Crossref
3. Hamedheidari S, Rafeh R. A novel agent-based approach to detect sinkhole attacks in wireless sensor networks. Elsevier Computers and Security. 2013; 37:1–14. Crossref
4. Kumar R, Arumugam U. Intrusion detection algorithm for mitigating sinkhole attack on LEACH protocol in wireless sensor networks. Hindawi Journal of Sensors. 2015; 1–12.
5. Jiao F, Dong L, Cui J, Xiang. Sinkhole attack detection based on redundancy mechanism in wireless sensor networks. Elsevier Procedia Computer Science. 2014; 31:711–20. Crossref
6. Shafieia H, Khonsaria A, Derakhshia H, Mousav P. Detection and mitigation of sinkhole attacks in wireless sensor networks. Elsevier Journal of Computer and System Sciences. 2014; 80(3):644–53. Crossref
7. Stafrace KS, Antonopoulos N. Military tactics in agent-based sinkhole attack detection for wireless ad hoc networks. Elsevier Computer Communications. 2010; 33(5):619–38. Crossref