An Improved Detection and Mitigation Approach of Sinkhole in Wireless Sensor Networks

Vishwas D B[1], Chinnaswamy C.N[2], Dr.T.H.Sreenivas [3]
[1]*PG student, CNE, Department of IS&E,*
The National Institute of Engineering, Mysuru, India
vishwasdb91@gmail.com
[2] *Associate Professor, Department of IS&E,*
The National Institute of Engineering, Mysuru, India
chinnaswamynie@gmail.com
[3]*Professor, Department of IS&E,*
The National Institute of Engineering, Mysuru, India

Abstract— *Nowadays wireless sensor network has gained a lot of importance in many areas, especially in military operations and monitoring applications. The size of the sensor nodes might range from that of a shoebox down to the size of a grain dust. These sensor nodes are vulnerable to various types of attacks, sensor nodes mainly sense the data and send it to the base station, during this transmission the major attack faced by the wireless sensor network is sinkhole attack, and presence of sinkhole node lure's all the network traffic away from the base station towards itself. Thereafter it can either alter the data packets or drop the packets without giving the base station a hint and finally destroy the network. Over the past years researchers have encouraged the use of mobile agents as a new and smart paradigm for distributed applications to overcome the limitations of sensor nodes. In order to detect the sinkhole attack it is required to do enhancement in routing algorithm, which uses mobile agents designed for wireless sensor networks.*

KEY WORDS— Mobile Agent, Sinkhole Attack, Wireless sensor Networks. NodeHashFunc, (AODV) Routing Protocol

1. INTRODUCTION

1.1. Wireless sensor network

Wireless Sensor Networks (WSNs) are used in many areas like military, ecological and health-related fields to perform various useful applications. These applications often include the monitoring of sensitive information such as enemy movement on the battlefield or the location of personnel in a building. In Wireless sensor networks (WSNs) forwarding of sensed data is done through multi-hop routing. Wireless sensor networks (WSNs) have drawn fair amount of research attention during last decade due to their varied application capability. The limited resources along with the hostile deployment environment of Wireless Sensor Networks (WSNs) put severe challenges to the research studies. Various aspects of such networks have been already studied and these types of networks are now well-established for many applications ranging from habitat monitoring to surveillance.

2. SINKHOLE ATTACK.

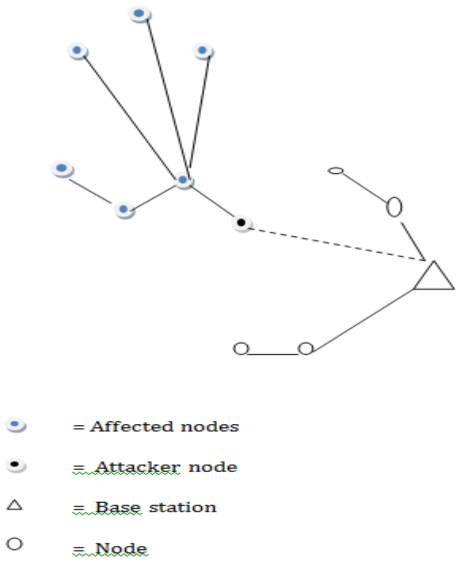


Fig 1: Example of a sinkhole attack in a Wireless Sensor Network

The sinkhole attack in WSN is that an intruder uses a compromised node in the sensor network of a particular area and lures some or all the traffic of that particular area and makes a sinkhole. The goal of a sinkhole attack is to misroute almost the whole traffic from a particular area (of the network) through acompromised node, Sinkhole attacks are carried out by making the compromised node look more attractive to all the neighboring nodes which have an effective routing path to the destination with high rate of energy.

For example that node may be any laptop with high energy and high performance power. First it just advertise that it have a high quality single hop connection with the BS to its neighboring nodes. After that all the nodes divert all their traffic to pass through the intruder node to the BS. Thus sinkhole attack is launched. Sinkholes attacks are difficult to be detected because of the routing information provided by each node are difficult to verify. Once the attacker made the sinkhole attack he can perform any type of attack in the WSN as the entire traffic flows through that sinkhole node so he can collect all the data through the node and misuse the collected data. He even drop all the packets or some of the packets also can perform Selective Forwarding attack, Wormhole attack, Flooding attack, Sybil attack, Black hole attack. Hence Sinkhole attack if not detected and mitigated at initial stage it may degrade the security of the Wireless Sensor Networks to a greater extent.

Sinkhole detection mobile agent based detection technique

In this technique we are using some unique codes (code1, code2 and code3), here code1 is the plain text, code 2 is the corresponding output obtained after performing the agent's hash function on code1, code 3 is a unique code used to interact with the valid node of the network. Due to nodes mobility, network maintenance phase should be done periodically during the network lifetime. Therefore, a malicious node can impersonate as a valid one and be placed in the neighbouring list of a node which is configuring its neighbouring matrix. Since the adversary does not know the time which a valid node is going to do the reconfiguration (i.e. updating neighbouring matrix), it should permanently listen to the network traffic, causing swift reduction in its energy and rapid incapability.

A node gives any information to a mobile agent and vice- versa only when the node and the agent trust each other. This trusting procedure is illustrated in Fig.2. As shown in Fig.2, a valid node contains the original codes code1 and code2 and, a valid agent contains code3 as well. Actually we use this procedure to detect the adversary nodes. The trusting procedure is as follows:

As shown in Fig.2, after an agent has placed on a node, it requests for code1 and produces code2 based on that by its unique hash function (i.e. AgentHashFunc ()), considered as step 1. In the next step, the agent submits code2 to the node. In case of being in accordance to the code2 stored in the node, it trusts the agent and produces code3 based on code2 using its unique hash function (i.e. NodeHashFunc ()). Now it is time for the agent to trust the node. In the last step of the trusting

procedure code3 is submitted to the agent. If it is equal to the one stored in agent source code, the agent will trust the node and submits the data code to it as well. Now there will be three situations according to the trusting

3. PROCEDURE:-

- Valid agent on a valid node: In this situation, after the agent has placed on the node, it requests for code1 and produces code2 as described before. Then the agent submits code2 to the node in the next step. Since the submitted code2 and the one stored in the node are the same, the node trusts the agent. In the next step, the valid node produces code3 based on code2 and submits it to the agent. Since this code is equal to the one stored in agent program, the agent trusts the node and gives the datacode to it.

- Valid agent on an adversary node: Similar to the previous situation the agent requests for code1 and produces code2 by its AgentHashFunc() method, submits it to the node and waits for the delivery of code3. But the node cannot submit the correct code3, since it does not have the original code1 and nodeHashFunc() method.

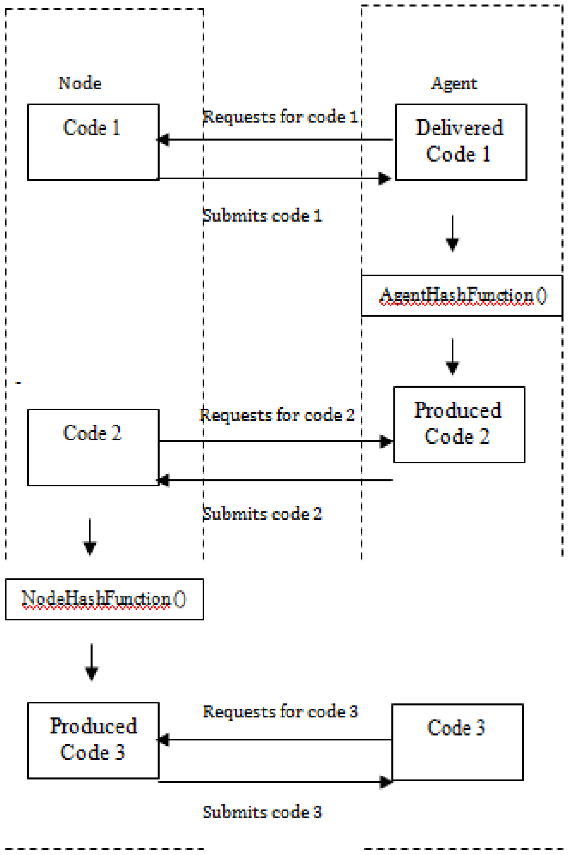


Fig 2: Trusting procedure of a mobile agent and a node

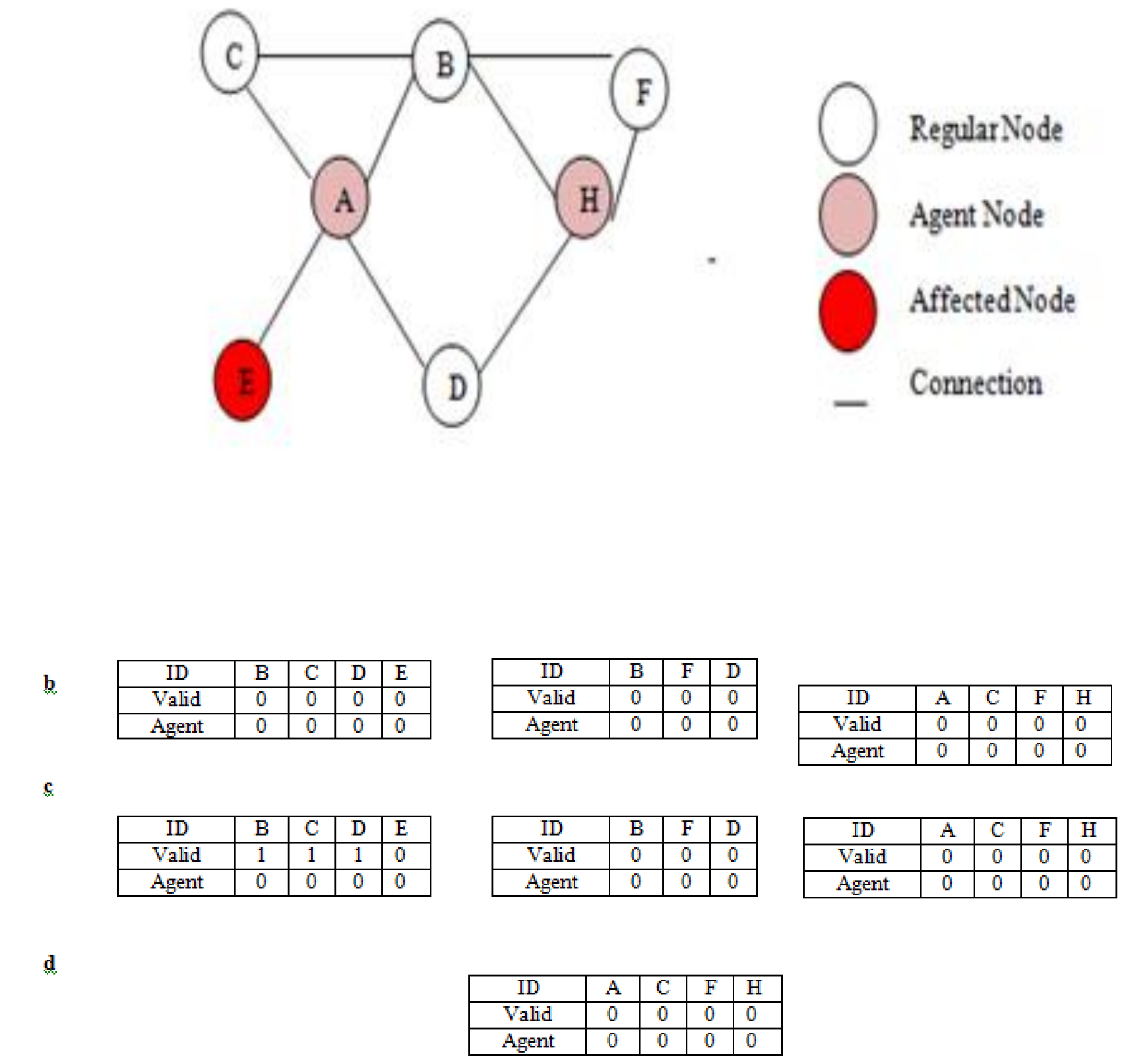
- Fake agent on a valid node: In this situation, after the fake agent has placed on the node and received code1, it will not be able to deliver the correct code2 to the node in the next step, because this agent does not have the original AgentHashFunc() method. Since this code is not the same as the one is stored in the node, it will not trust the agent and the agent will be ignored as well.

4. SINKHOLE MITIGATION

The algorithm used for mitigation of sinkhole is formed of two phases: network deployment phase tells how the network is configured and network maintenance phase indicates how to keep the network safe:

4.1. Network Deployment Phase

At first nodes are uniformly distributed in the network. Then the base station randomly chooses a number of nodes based on a desired percentage of mobile agents to send them the agent packets. When a node receives an agent packet from the base station, it becomes an agent node. After this step, to create the neighboring matrix, all nodes broadcast HELLO packets to find nodes in their radio frequency range. It is obvious that malicious nodes can put themselves into neighboring matrix as well. After neighbor finding process, each entry of neighboring matrix contains the ids of single hop. Neighbor nodes but agent bit and valid bit are still false. A wireless sensor network is shown in Fig. 3a in which nodes A and H have agents and E is a malicious node. Fig. 3b depicts nodes A, H, and B neighboring matrix after sending HELLO packets. As shown in the illustration, in this step all neighbor nodes in the range are found which include malicious ones as well.



b

ID	B	C	D	E
Valid	0	0	0	0
Agent	0	0	0	0

ID	B	F	D
Valid	0	0	0
Agent	0	0	0

ID	A	C	F	H
Valid	0	0	0	0
Agent	0	0	0	0

c

ID	B	C	D	E
Valid	1	1	1	0
Agent	0	0	0	0

ID	B	F	D
Valid	0	0	0
Agent	0	0	0

ID	A	C	F	H
Valid	0	0	0	0
Agent	0	0	0	0

d

ID	A	C	F	H
Valid	0	0	0	0
Agent	0	0	0	0

Fig 3: Illustration of the algorithm

4.2. Network Maintenance Phase

After network deployment phase was done, the agents start agent cycling. But before giving any information to a node or receiving from it, a three-step negotiation referred to as

'Trusting Procedure' is done between the agent and the node.

This negotiation will be explained in Section 3.5. The node being trustable, interactions begin; otherwise, it is considered an attacker. If the neighbour node is trustable, on the agent returning to the original node (or agent node), its corresponding valid bit in the neighbouring matrix is changed to true (i.e. one), or else, remains false (i.e. zero); moreover, if the neighbour node is an agent node, its agent bit becomes true as well. Since only a few percent of nodes have agents (i.e. are agent nodes), after the determination of neighbours' validity, agent nodes multicast a packet e named 'trust packet' e to all its trustable neighbours which do not have agents in order to inform them of the trustable and, malicious nodes. In addition, since the nodes are moving, when an agent comes back to the agent node, the received signal strength is calculated.

If it is less than a threshold, the neighbor node will be removed from the neighboring list; assuming it is moving away. If the agent bit of the removed node is false, the agent node sends to it a control packet to do the neighbor finding process again, because it has no agent and may not be under the cover of any mobile agent either. Fig. 3c depicts neighbor matrix for nodes A, H, and B after agent migration. Valid and agent bits are filled with relevant values. But since node B does not have agent it lacks information about nodes C and F. So agent nodes (in here A and H) multicast trust packets to their trusted neighbors such as B. After receiving trust packets, node B updates its matrix, which is shown in Fig. 3d.

5. RELATED WORK

Tejinderdeep Singh and Harpreet Kaur Arora [4] proposed a solution for Sinkhole attacks detection in WSN using Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol. This system consists of three steps. The sender node first requests the sequence number with the rreq message, if the node replies its sequence number with rrep message. Transmitting node will match sequence number in its routing table. If matches then data will be shared otherwise it will be assign the sequence number to the node. If the node accepts the sequence number then the node will enter in the network otherwise it will be eradicated from the network.

D. Sheela., et al., [5] proposed routing algorithm based on mobile agents to defend against sinkhole attacks in WSN. Mobile agent is a self controlling software program that visits every node in the network either periodical or on required. By using the collected information the mobile agents make every node alert of the entire network so that a valid node would not listen to the wrong information from malicious or compromised node which leads to sinkhole attack. The important feature of the proposed mechanism is that does not require any encryption or decryption mechanism for detecting the sinkhole attack. Very less energy is enough for this mechanism than the normal routing protocols.

6. FUTURE ENHANCEMENT

In addition to the mentioned approach we can introduce a new method of identifying threshold value for finding malicious node especially to detecting sinkhole attack. Giving more focus on how to improve packet transmission from source to destination securely by doing enhancement in routing algorithm based on mobile agents against sinkhole attack. Proposed routing algorithm uses mobile agents to collect the network connection information to build the global information matrix of nodes by which data packets are routed and transferred. Then, detect the sinkhole node based on difference of source sequence number of current and previous request using threshold value. This proposed approach is well used not only avoiding sinkhole attack but also used to detect the sinkhole node in the network precisely.

7. CONCLUSION

In This paper we have proposed an efficient mobile agent based approach to detect and mitigate sinkhole attacks in a wireless sensor network with mobile nodes. We used mobile agents to detect attacker nodes and trusted neighbors in order to inform nodes from their environment. The proposed approach helps to reduce the memory overhead of the nodes in the network. From the point of energy utilization, it is economic, because only an agent with very small database is transferred to detect malicious nodes. Here the expense of using public keys and private keys is eliminated hence no cryptographic overhead. Hence in future we are going to increase the performance of our algorithm and decrease the average uncovered nodes by mixing it with other techniques and we will try to extend our algorithm to cope with other attacks in wireless sensor networks.

8. REFERENCES

[1] Sina Hamedheidari and Reza Rafeh "A novel agent-based approach to detect sinkhole attacks in wirelss sensor networks," Computer and Security 37 (2013) I-I4

[2] H.Shafiei, A.Khonsari, H.Derakhshi and P.Mousavi "Detection and mitigation of sinkhole attacks in wireless sensor networks," Journal of computer and System Sciences 80 (2014)644-653

[3] Vandana Salve, Leena Ragha, Nilesh Marathe "An enhanced secure routing algorithm against sinkhole attack in wireless sensor networks," International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106, Volume-2, Issue-8, Aug.-2014

[4] Tejinderdeep Singh and Harpreet Kaur Arora, "Detection and Correction of Sinkhole Attack with Novel Method in WSN Using NS2 Tool", International Journal of Advanced Computer Science and Applications, Vol. 4, No. 2, 2013, pp 32-35.

[5] D. Sheela, et al, "A non Cryptographic method of Sink hole attack Detection in Wireless Sensor Networks", IEEE-International Conference on Recent Trends in Information Technology, June 3-5 2011, pp 527-532,