Volume 5, Issue 8, August 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review on Impact of Sinkhole Attack in Wireless Sensor Networks

Amrit Pal Singh[1], Parminder Singh[2], Rakesh Kumar[3]
[1, 2] Department of Information Technology, CEC, Landran, Chandigarh, India
[3]Department of Computer Science, Sachdeva Engg. Colege for Girls, Kharar, Chandigarh, India

Abstract----Wireless Sensor Networks (WSNs) are widely used in many areas, like in military operations and monitoring applications. Their wireless nature makes them very attractive to attackers, so its security system plays a vital role. Due to the limitations on resources, such as energy and storage, the security mechanism of WSNs have to be considered differently from traditional networks. 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 this paper we are using clustering technique along with replicated mobile agents to prevent the wireless sensor network from sinkhole attacks. We use mobile agents to aware every node from its trusted neighbors so they do not listen to the traffics generated by malicious nodes. We evaluate our work in terms of packet loss rate, throughput and end to end delay.

Keywords— AODV, RREQ, RREP, Sink node, Throughput.

I. INTRODUCTION

A. Wireless Sensor Network

The recent drive in the information technology industry toward new wireless communication devices and systems and their utilization in addressing a wide variety of real-world problems have resulted in several new areas of active research, wireless sensor networks being one such hot topic. The Internet has been able to provide a large number of users with the ability to move diverse forms of information readily and thus revolutionized business, defense, education, industry, research, and science. Sensor networking may, in the long run, be equally significant by providing measurement of the physical phenomena around us, leading to their understanding and ultimately the utilization of this information for a wide range of practical applications. Potential applications of sensor networking include defense, environmental and habitat monitoring healthcare monitoring transportation manufacturing and search and rescue. Wireless Sensor Network has the potential for many applications[1] e.g. for military purpose, it can be use for monitoring, tracking and surveillance of borders, in industry for factory instrumentation, in a large metropolis to monitor traffic density and road conditions, in engineering to monitor buildings structures, in environment to monitor forest, oceans, precision agriculture.

Wireless Sensor Networks can be categorized as structured and unstructured [2]. Unstructured wireless sensor network contains dense collection of sensor nodes. Sensor nodes are deployed in ad-hoc manner. In unstructured wireless sensor network, maintenance is difficult because of dense deployment of sensor nodes. Structured wireless sensor network contains sensor nodes that are deployed in a pre-planned manner. Management cost is low and maintenance is easy for structured wireless sensor network because of less sensor nodes deployed. Depending upon whether sensor nodes have same capabilities, wireless sensor network can be categorized as homogenous and heterogeneous [3]. In homogenous sensor network all nodes have same capabilities in terms of energy, processing power and memory. In heterogeneous sensor networks, some special sensor nodes are equipped with more processing and communicating capabilities.

B. Applications

WSNs have profound effects on military and civil applications[4] such as target field imaging, intrusion detection, weather monitoring, security and tactical surveillance, distributed computing, detecting ambient conditions such as temperature, movement, sound, light, or the presence of certain objects, inventory control, and disaster management. Wireless sensor network is an emerging class of networks which can be used to monitor an object, area or both [5]. Object monitoring involves structural monitoring, medical diagnostics, urban terrain mapping etc. Area monitoring involves military surveillance, environment surveillance [6], habitat monitoring etc.

C. Characteristics [7]

- Small-scale sensor nodes
- Limited power they can harvest or store
- Harsh environmental conditions
- Mobility of nodes

- Heterogeneity of nodes
- Large scale of deployment
- Unattended operation

WSN has some unique features [8] compared to the traditional single hop network:

(1) The network has not a fixed strict control center; all nodes enter or exit the network coequally.
(2) All nodes can form a private network based on a certain protocol automatically.
(3) All nodes can work as a router and communicate with each other via intermediate nodes with several hops.
(4) The network has s dynamic topology.

D. Attacks [8] on WSNs

1. Tampering: - In tampering attacker may damage a sensor node, replace the entire node or part of its hardware or even electronically interrogate the nodes to gain access to sensitive information, such as shared cryptographic keys and how to access higher communication layers.
2. Selective forwarding: - In such an attack the adversary includes itself in a data flow path of interest. Then the attacker may choose not to forward certain packets and drop them causing a sort of black hole.
3. Sybil Attack: - A malicious node presents multiple identities to the network is called Sybil attack. This attack is especially confusing to geographic routing protocols as the adversary appears to be in multiple locations at once.
4. Jamming: - it interferes with the radio frequencies of the sensor nodes. Only a few jamming nodes can put a considerable amount of the nodes out of order. If the adversary can block the entire network then that constitutes complete DoS.
5. Wormhole Attack: - In this malicious node create a path between the network and it shows that it is the shortest path so the base station send data through it and the data got lost.

E. Sinkhole Attack

The goal of a sinkhole attack is to misroute almost the whole traffic from a particular area through a compromised node. Sinkhole attacks typically work by making a compromised node looking especially attractive to surrounding nodes with respect to the routing algorithms, such as AODV. Fig. 1 shows an example of a sinkhole attack where a compromised node attracts surrounding nodes with fake routing information, and then alters the data passing through
It or performs selective forwarding. The sinkhole attack prevents the base station from obtaining complete and correct sensed data, and thus leads to a serious threat.

We are using Ad hoc On Demand Distance Vector (AODV) as our routing protocol, it will be explained how a sinkhole attack is launched in this protocol. In order to find the path to the base station, a node will multicast route request (RREQ) packets to it single hop neighbors. When a neighbor node receive request, if it has direct path to base station it will multicast route reply (RREP) packet or else it will send RREQ to its neighbor to continue route finding process. RREQ and RREP packets in AODV are equipped with hop count, so an adversary node can affect the hop count to attack the network.

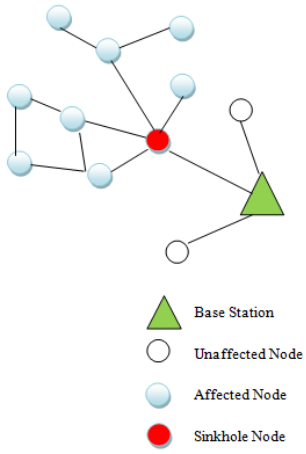

Fig. 1 Example of Sinkhole attack in Wireless Sensor Network.

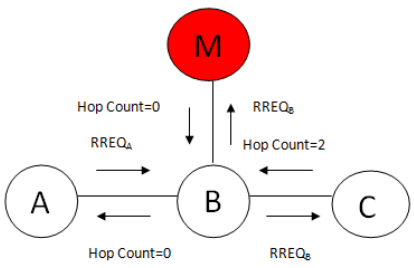

Fig. 2 A sample sinkhole attacks with modified hop count value in AODV routing protocol.

Now Fig. 2 shows how a malicious node modified the hop count to attack the network. Here malicious node sends lesser hop count to node B, to show it is the shortest path. Thus node A assumes that the route through M is the shortest and sends the data through it. In this way sinkhole attack is achieved.

II. RELATED WORK

Intrusion detection has long been an active research topic in the network evolution. Recently, many techniques have been introduced to detect and prevent the sinkhole attack in wireless sensor networks. The study by (Stefan K. Stafrace and Nick Antonopoulos, 2010) provides military tactics along with mobile agents are used to detect sinkhole attacks in wireless network. Recently we are using agent based IDS to detect sinkhole attacks but in this paper it proposed a approach in which it is using military tactics along with agent based IDS to detect sinkhole attacks in wireless network. A regular patrolling is going on of the network and the risk factor is associated with it. Whenever the risk is high i.e. the sinkhole attack has detected we can easily prevent it by using the check points. In (P. Samundiswary and Dananjayan, 2010) a secured path redundancy algorithm has been applied to implement in heterogeneous sensor networks by using alternate path scheme in these networks with mobile nodes for mobile sinks to defend against sinkhole attacks. This proposed approach is not suitable for homogenous sensor networks. In (D Sheela and Mahadevan, 2011) they introduced mobile agents to detect the sinkhole attack in wireless sensor networks. But in this as the number of nodes increases the overhead of the network also decreases that degrade performance of the network. In (Sina Hamedheidari and Reza Rafeh, 2013) they provide a mobile agent based approach to detect and prevent the sinkhole attacks in wireless sensor networks. They used mobile agents to detect malicious nodes and trusted neighbors in order to inform nodes from their environment.

III. CONCLUSION AND FUTURE WORK

WSNs have many characteristics that make them very vulnerable to malicious attacks in hostile environments. A wireless channel is open to everyone. With a radio interface configured at the same frequency band, anyone can monitor or participate in communications. This provides a convenient way for attackers to break into WSNs. In the current paper we have presented the impact of Sinkhole attack. In future we will present the concept of replicated agent to prevent and control the impact of Sinkhole attack.

REFERENCES

[1] Marcos Augusto M. Vieira, Claudionor N. Coelho. Jr" Survey on Wireless Sensor Network Devices", IEEE, 2003, pp. 537-544.
[2] J. Yick, B. Mukherjee, D. Ghosal, "Wireless sensor network survey", Computer Networks, vol. 52, no. 12, 2008, pp. 2292-2330.
[3] H. Nakayama, N. Ansari, A. Jamalipour, Y. Nemoto, N. Kato, "Fault-resilient sensing in wireless sensor networks", Computer Communications, vol. 30, no. 11, 2007, pp. 2375-2384.
[4] Jamal N.Al-Karaki and Ahmed E.Kamal," Routing techniques in wireless sensor networks: A Survey", IEEE Wireless Communications, Dec 2004, pp. 6-28.
[5] D. Culler, D. Estrin, M. Srivastava, "Overview of sensor networks", IEEE Computer, vol. 37, no. 8, 2004, pp. 41–49.
[6] R. Holman, J. Stanley, T. Ozkan-Haller, "Applying video sensor networks to near shore environment monitoring", IEEE Pervasive Computing, vol. 2, no. 4, 2003, pp. 14-21.
[7] Sameer Tilak, Nael B. Abu-Ghazaleh and Wendi Heinzelman," A Taxonomy of Wireless Micro-Sensor Networks Models", Vol 1, pp. 1-8.
[8] Dunfan Ye, Daoli Gong and Wei Wang," Application of wireless sensor network in Environmental Monitoring", 2009, pp. 205-208.
[9] Vinay Soni, Pratik Modi and Vishvash Chaudhri," Detecting Sinkhole Attack in Wireless Sensor Network", Vol 2, Feb 2013, pp. 29-32.
[10] Sina Hamedheidari and Reza Rafeh "A novel agent-based approach to detect sinkhole attacks in wireless sensor networks" computer and security 37, 2013, pp. 1-14.
[11] Stefan K. Stafrace , Nick Antonopoulos" Military tactics in agent-based sinkhole attack detection for wireless" Computer Communications 33, 2010, pp. 619–638.
[12] P.Samundiswary and Dananjayan,"Detection of sinkhole attacks for mobile nodes in heterogeneous sensor network with mobile sinks", 2010, pp. 127-133.
[13] D. Sheela and Dr. G.Mahadevan," A non cryptographic method of sinkhole attack detection in wireless sensor networks", 2011, 527-532.
[14] Karlof C, Wagner D," Secure routing in sensor networks: attacks and countermeasures", 2003, pp. 113-127.
[15] Maninder Kaur, Parminder Singh, "A Mathematical Approach to Avoid Congestion and To Analyze Snoop Behavior In Wired Cum Wireless Network" IJEAT 2012.pp 347-352.
[16] Parminder Singh, "Comparative study between unicast and Multicast Routing Protocols in different data rates using VANET", IEEE, 2014, pp. 278– 284.
[17] Parminder Singh, "Design an Framework of Wireless Sensor Networks by Preventing Malicious Nodes Attack", International Conference Elsevier, 2014,pp.195-200.

