iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 Issue: VII Month of publication: July 2019

DOI: http://doi.org/10.22214/ijraset.2019.7072

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue VII, July 2019- Available at www.ijraset.com

Attacks on Wireless Sensor Networks: A Survey

T. Daniel Prasanth[1], Reshma[2], M. Shalemu Raju[3]
[1, 2]Ramachandra College of Engineering, Dept.of Computer Science and Engineering, Eluru, India.
[3]Vizag Institute of Technology, Dept. of Electronics and Communication Engineering, Dakamarri, India.

Abstract: A large number of sensor nodes having limited memory capacity, computing power and having networking capabilities are used to gather sensing information-the entire sensor node network is collectively called as a Wireless Sensor Network. The limited operational design of wireless sensor network makes it vulnerable to various attacks such as a sinkhole attack, clone attack etc. This paper focuses on exploring the constraints that lead to sinkhole attack, clone attack in wireless sensor network.

Keywords: Wireless sensor network, TinyAODV, Sinkhole attack, Clone attack.

I. INTRODUCTION

Interacting with environment embedded devices is very essential for monitoring and recording the environment physical conditions. The data is gathered using small sensors having network capabilities and they act as nodes. Information is processed by the nodes and is communicated to a base node which analyzes the information and there by making use of it.

II. LITERATURE SURVEY

The sensor nodes along with base node constitute wireless sensor network. A wireless sensor network comprises of small sensor nodes and transmitting information among themselves[1] with the help of radio signals . wireless sensor network constitute diversified range of applications like transportation, infrastructural, military. Wireless sensor network uses protocols that require less power consumption. wireless sensor network devices usually have low memory, low computational power and an operating distance of around 100mts[2]. In a Wireless sensor network the nodes communicate using different protocols like Mini-route protocol, Tiny AODV protocol. Optimized to give better results for sensor network . The individual sensor nodes send information to the base node using the protocols designed for wireless sensor network. The protocols are designed in such a way that low memory and low powered devices can communicate effectively which paves the way for intrusion, since the wireless sensor network have limited memory, computing power they cannot handle normal cryptography and statistical computations which require a considerable amount of processing power, which is unavailable in sensor networks. There by enabling an insider or outside to gain access to a node[3] and eventually gaining access to the whole network.and example of such an attack is a sink hole attack.

III. CHALLENGES FACED BY WIRELESS SENSOR NETWORKS

1) *Limited Power Resources:* An advantage of a wireless sensor network is independent of wiring costs which makes it suitable for deployment in subtle environments to gather, monitor information. Remote deployment is the reason why wireless sensor network have limited power resources which makes the battered power to be consumed more efficiently, so the routing protocols must use less power and should be quick, this make it more prone to attacks since the routing protocols are nor strong enough.
2) *Location of Sensor Nodes:* Wireless sensor network can be deployed underground, underwater, inside vehicles, on mountains etc. which are not reachable by humans round the clock. Once installed they might be unattended for days, months depending on the mode of deployment which makes it easy for outsiders to physically or wirelessly gain access to a node which in turn brings down the entire network.
3) *Low Computational Functionaries:* As most of the wireless sensor network doesn’t involving physical wiring harness for functioning they use battery, hence sensors use system-on-chip that require less power are used on board, such devices have low computing power, which makes it difficult for securely verifying a node[4], there by exposing a node easily to the attacker.
4) *Network Size:* In a wireless sensor network there can be any number of sensor nodes that gather information,depending on the mode of usage there can be less number of attacks when there are less number of nodes, but as nodes increases the network size increases it will be difficult to maintain all nodes securely and hence making the attacker easy to gain access to a node.
5) *Data Transfer Path:* Sensor nodes in a wireless sensor network communicate the gathered information wirelessly, the information is passed through multiple nodes[5] before it reaches base node. An attacked node can advertise itself as the node nearest to the base node, which makes all the nodes believe the malicious node, there by compromising the information pattern .

6) *Geographical Location of a Node:* As wireless sensor network are deployed onto a wide geographical locations which cannot be continuously taken care of they can be physically accessed by outsiders who will in turn extract node information and might even replace a node having the same identical features so as to attack the network

IV. ATTACKS ON WIRELESS SENSOR NETWORKS

1) *Sink Hole Attack:* In sink hole attack either insider or an outsider gains access to a sensor node and gives out false routing information[6] to other nodes like advertising fake routes to its neighbouring nodes leading to an virtual inconsistency in routing information, which makes the attacked node as legitimate node and the nearest node to the base station. An AODV protocol implemented in a wireless sensor network network and a compromised node advertises itself as the node nearest to the base station by sending wrong information to the neighbouring nodes can be seen in fig 1.

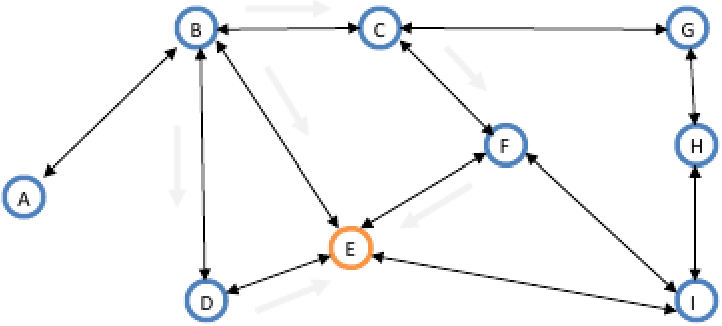

Fig. 1 A Sink hole attack with E as a compromised node

When node B is ready to send data to a destination node H, node B sends RREQ to its neighbours, each neighbour of B sends RREQ to their neighbours till node H is reachable. E doesn’t send RREQ to I or F but replies with RREP to B, hence making B to think E is the nearest neighbor to H.In this way E advertising itself as the nearest neighbor to H , there by making B pass all its packets to E, hoping E is the nearest neighbor to H. But in reality E is a compromised node reading all the packet information from B.

2) *Clone Attack:* In Clone attack an attacker gains physical access to a node, collects the credentials, with the information gathered a new node with the same specifications is deployed into the network, the cloned node misinforms the network as a legitimate node, the cloned node might be used to generate false data[7] which might disrupt the working of devices that depend on a wireless sensor network. The attacker can also use cloned node to devise other attacks on a wireless sensor network.

TABLE I
Attacks on Wireless Sensor Networks and workarounds

Attack	Cause	Solution
Sink Hole attack	Under optimized routing algorithms.	Hop Count monitoring[8], Intrusion Detection system[9].
Clone attack	Location of sensor node in remote areas, poor security.	Cloned key detection protocol[10], Distributed protocols[11].
SYN flooding	High channel error rate. No mechanism to distinguish whether a congestion or attack was the reason for a packet loss.	Filtering, Firewalls.
Session hijacking	Spoofing IP address.	Hash chain numbering.
Denial of service	Signal jamming. Using capture effect of malicious nodes.	Using spread spectrum communication technique.

V. CONCLUSION AND FUTURE WORK

Wireless sensor network are capable of working in ambient conditions responsible for measuring responses, in different physical conditions which makes them more prone to attacks. Information gathered can be effectively and securely routed using advanced algorithms but at the cost of network size and processing capabilities as the network size increases most of the algorithms underperform. Future solutions must focus on increasing computational power, low powered cryptography algorithms that can be fit into low memory sensor nodes.

REFERENCES

[1] Jennifer Yick, Biswanath Mukherjee, DipakGhoshal,"Wireless sensor network survey", www.elsevier.com/locate/comnet, April 2008, pp. 2292–2330.

[2] W. T. Zhu, J. Zhou, R. H. Deng, and F. Bao, "Detecting node replication attacks in wireless sensor networks: a survey," Journal of Network and Computer Applications, vol. 35, no. 3, pp. 1022–1034, 2012.

[3] C. Hartung, J. Balasalle, and R. Han, "Node compromise in sensor networks: the need for secure systems," Tech. Rep. CU-CS-988-04, Department of Computer Science, University of Colorado at Boulder, 2004.

[4] 444.Fei Hu and Neeraj K. Sharma, "Security considerations in ad hoc sensor networks", Ad Hoc Networks, Published by Elsevier Science, 2005, pp. 69–89.

[5] Perrig, Adrian, John Stankovic, and David Wagner. "Security in Wireless Sensor Networks", Communications of the ACM, Volume 47, 2004, pp. 53-57.

[6] VinaySoni, Pratik Modi, VishvashChaudhri," Detecting Sinkhole Attack in Wireless Sensor Network", International Journal of Application or Innovation in Engineering & Management (IJAIEM),Volume 2, Issue 2, February 2013,pp:29-32.

[7] H. Choi, S. Zhu, and T. F. L. Porta, "SET: detecting node clones in sensor networks," in Proceedings of the 3rd International Conference on Security and Privacy in Communication Networks (SecureComm '07), pp. 341–350, September 2007.

[8] Daniel Dallas, Christopher Leckie, Kotagiri Ramamohanarao; "Hop-Count Monitoring: Detecting Sinkhole Attacks in Wireless Sensor Networks" 15th IEEE International Conference on Networks, 2007, ICON 2007, pp. 176-181.

[9] Edith C. H. Ngai, Jiangchuan Liu and Michael R. Lyu; "On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks" IEEE International Conference on Communications, 2006, Volume 8, pp. 3383- 3389.

[10] R. Brooks, P. Y. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M. T. Kandemir, "On the detection of clones in sensor networks using random key predistribution," IEEE Transactions on Systems, Man and Cybernetics C, vol. 37, no. 6, pp. 1246–1258, 2007.

[11] B. Zhu, S. Setia, S. Jajodia, S. Roy, and L. Wang, "Localized multicast: efficient and distributed replica detection in large-scale sensor networks," IEEE Transactions on Mobile Computing, vol. 9, no. 7, pp. 913–926, 2010.