Volume 9, Special Issue No. 1, February 2018

ISBN: 978-93-5300-455-2

International Journal of Advanced Research in Computer Science
(ISSN: 0976-5697)

REVIEW ARTICLE

SHRI SHANKARLAL SUNDARBAI SHASUN JAIN COLLEGE FOR WOMEN
ICRACC 2018
(23rd–24th February 2018)

Available Online at www.ijarcs.info

A Study Paper on Wireless Sensor Secure Routing

T. Yegammai,
Assistant Professor, Department of Computer Science,
yegammai@shasuncollege.edu.in

S.G Packiavathy
Head, Department of Computer Applications,
packiavathypaul@hotmail.com

ABSTRACT

An important purpose is that the wireless sensor routing security networks have many sensor routing protocols and nodes but have no security. Security goals for routing in sensor networks show us how crippling attacks have been made and attacks have been made and attacks against ad-hoc and peer-to peer networks. Two undocumented attacks such as sinkhole and hello floods which have been described and analyze the security of all secure routing in wireless sensor networks and protocols used for disseminating controls and information's network called sinks.

INTRODUCTION:

Routing security in wireless networks is an important purpose in the routing network which has limited nodes and application networks but have no security. Although there is no security available, we make the security properties. In insecure wireless communication, limited nodes[1] and insider threats, where when designing the network secure routing adversary people has laptops with energy and long range communication, where the routing becomes non-trivial. Crippling attack is provided for all the major routing protocols because they have no security on the routing of sensor network and is insecure.

BACKGROUND:

Sensor network refers to the sensors and general computing elements. A sensor network consists of hundreds and thousands of low power costs and nodes but only at fixed locations which affects the environment[2]. The sensor networks which consist of one or more point of control is the base stations. The sensor node is the access point for the securing routing which is used to disseminate the control information on networks. Sensor network routing might have laptop, memory- storage, and high-bandwidth links for communication among the sensor network. Sensor network use low power and bandwidth that would communicate to the nearest base station for sensor network. The aggregation networks where the total numbers of messages sent, the energy is saved in the network where from the aggregation point they collect the readings from surrounding nodes. Sensor networks differ from other systems where it has a great challenge [2]. The value of sensor networks comes from many nodes where they will have to develop cheaper sensor nodes. Security is critical when networks are at risk where we have sensor nodes such as[3]:- High bandwidth Sensor node Base station Low latency and Only laptop and base stations use low latency and high bandwidth.

RELATED WORK:

Security issues are similar to sensor networks and are developed for ad-hoc networks. The secure routing protocols [4] for ad-hoc networks and sensor network reasons are that they sense security in ad-hoc network for authentication and secure routing protocols. The routing protocols are based on public key cryptography[5] which is used for sensor nodes.

SECURITY GOALS:

Secure routing protocols which have integrity, power and availability of messages in presence of arbitrary power. Security is not relevant to the application data and not responsible for routing protocol.

ATTACKS ON SENSOR ROUTING:

There is attack against the ad-hoc sensor networks but quite simple for the following categories:

SINK HOLE:

The goal is to take away all the traffic (nodes) from the particular area through nodes creating a sinkhole with adversary at the centre [5]. Sinkhole attacks which enables many other attacks where only one single node provides single high quality information which influences large number of nodes. The laptop class with transmitter which provides a high quality route for transmitting with power.

HELLO FLOOD:

The hello packets which are available to the bound channel are available to the attackers. An advisory situated close to the base station may be completely disrupted[8]. Protocols which depend on the local information exchange between neighboring nodes for maintenance nodes.

Attacks on specific sensor network protocols:

The main attacks of the sinkhole and hello flood is that the tiny OS protocols which can increase latency or disable thread [7]. The attacks on the link and sensor networks are against the network routing by line layers encryption. Sinkhole attacks on the network. Protocols which defend against protocols and the provided information, such as

HELLO FLOODS ATTACKS:

The hello floods attacks which verify the links of the nodes based on messages over the link. The hello floods attacks verify the link between two nodes, even if the advisory has high sensitive networks which will verify neighbors for each node to prevent hello flood attack.

CONCLUSION:

Securing routing which becomes vital to acceptance and the use of sensor networks against various protocols and attacks against the ad-hoc and peer to peer network where the attacks and routing protocols which defeat the security goals against the adversary. But we have demonstrated the currently routing protocols against the sinkhole and hello flood attacks. A design of the sensor network routing protocols which satisfies the security goals and also where the authentication and sensor routing protocols which can be used as security nodes and where the key cryptography which cannot depend the laptop class adversary and the protocol can be designed well for sensor network to be secured.

REFERENCES

[1] Y.-C. Hu, A. Perrig, and D. B. Johnson, “Wormhole detection in wireless ad hoc networks,”Department of Computer Science, Rice University, Tech. Rep. TR01-384, June 2002.

[2] V. D. Park and M. S. Corson, “A highly adaptive distributed routing algorithm for mobile wireless networks,” in *IEEE INFOCOM ’97*, 1997,pp. 1405–1413.

[3] D. B. Johnson and D. A. Maltz, “Dynamic source routing in ad hoc wireless networks,” in *Mobile Computing*, Imielinski and Korth, Eds. Kluwer Academic Publishers, 1996, vol. 353.

[4] F. Stajano and R. J. Anderson, “The resurrecting duckling: Security issues for ad-hoc wireless networks,” in *Seventh International Security Protocols Workshop*, 1999, pp. 172–194.

[5] J. Hubaux, L. Buttyan, and S. Capkun, “The quest for security in mobile ad hoc networks,” in *Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC 2001)*, 2001.

[6] L. Zhou and Z. Haas, “Securing ad hoc networks,” *IEEE Network Magazine*, vol. 13, no. 6, November/December 1999.

[7] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, “Providing robust and ubiquitous security support for mobile ad-hoc networks,” in *ICNP*, 2001,pp. 251– 260.