www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 6 June 2015, Page No. 12266-12268

Survey on security and privacy issues of Wireless Sensor Network

Seema Mane, Madhur Patrikar
Email:seemamane491@gmail.com
Department of Computer Engineering, Maharashtra Institute of Technology, Pune 411038, India
Email:mapatrikar@gmail.com
Department of Computer Engineering, Maharashtra Institute of Technology, Pune 411038, India

***Abstract*- Proliferation of Wireless sensor network is increased. Security, how to localized sensor between two nodes, efficient authentication, privacy, scalability, flexibility and availability, these are main issues of wireless sensor network. Clustering based wireless sensor network will solve the problem of security, privacy issues and scalability.**

Keywords: wireless sensor network; clustering; jammer; vampire attack

I. INTRODUCTION

Security problem is one of the important issue for Wireless Sensor Network. The paper focuses on the security and privacy issues of WSN applications. One of the most needed and challenging components in a wireless sensor network is how to localize sensor in the network.WSN is type of computer network where in radio waves is used to connect electronics devices with internet. WSN are broadly categorized into two types: static and dynamic depending on the nature of the topology of network used in WSN. To discover the sensor positions in a secure and effective manner, node identification and distance estimation are needed. Availability is one of the issues of WSN. Vampire attacks are not depending on protocols, they are based on general properties of protocol such as link, state, distance, rout etc.

Vampires use protocol-compliant messages, these attacks are difficult to detect and prevent also.

II. RELATED WORK

Shih-Chang Lin and Chih-Yu Wen proposed a device based ranging and node based identification scheme to improve the reliability we should focused on how and when to locate sensor between two nodes and how to provide security to the sensor networks. They analyzed physical property of a device, different type of delays such as communication delay, internal component delay, difference of the clocks, and response delay between two wireless sensors based on that information. They identify first to wireless sensors and then to renew the network node information. They proposed asynchronous ranging based device and used node identification algorithm for identifying malicious sensor nodes in the network and it is best suited to the resilient clock synchronization scheme to the successful detection rate of antinodes and ranging accuracy. [5]

When two nodes are communicated with each other via router or any access media, then security can be compromised. Eugene Y. Vasserman and Nicholas Hopper explore resource depletion attacks at the routing protocol layer, which disable networks by using battery power. These types of attacks rely on the properties of classes of routing protocols. The protocol is used to detect vampire attacks also. The quality of the protocol is depending on number of nodes. To prevent from vampires they do not allowed backtracking to search the node [6].

Yi-Shing Liou, Rung-Hung Gau and Chung-Ju Chang, proposed algorithms for medium access control in wireless networks. The proposed algorithm takes the input from information theoretic capacity area of a multiple access channel. According to the algorithms, a node is dynamically adjusted by using the previous strategies of other nodes and the channel feedback. Transmission threshold and an aggression level are composedly used in the strategy. Algorithm of symmetric learning for maximizing throughput and to maintain balance between throughput and fairness. A

novel methods is used to properly choose a finite number of available data on transmission rates [7].

The losses are caused by link errors only, the combined of link errors and malicious drop. Conventional algorithms which used detecting the packet loss rate cannot gives satisfactory result for detection accuracy. The detection accuracy is improved by a homomorphic linear authenticator (HLA). HLA used public auditing architecture and allows the detector to verify the packet loss information send by nodes. To reduce the computation overhead of the baseline scheme, a packet block based mechanism is used, which allows one to trade detection accuracy for lower computation complexity. It gives better detection accuracy than conventional methods such as a maximum-likelihood based detection [2].

Caching is to store parts of the mostly used content by users in end users' memory and its help to reduce peak data rates. Considered the secure caching problem. The goal of problem is to minimized leakage or information loss. It was more secure for memory storage and in low cost, they achieved good transmission rate. It is shown that the rate achieved by the proposed caching scheme with secure delivery is within a constant multiplicative factor from the information-theoretic optimal rate for almost all parameter values of practical interest [3].

III. ISSUES AND METHODS OF WSN

1. *Distribution scheme*: A distributed scheme for secure ranging and node identification, applying the device physical characteristics to locking the information, and the response delay time, the DARNI (Device-based Asynchronous Ranging and Node Identification) can be used to detect misbehavior of anti-nodes. It solved anti-node verification problem without changing any hardware and software infrastructure and reliably provide a secure distance measurement system in wireless sensor. We should require focusing on the methods to design energy efficient message to improve like DARNI method. Clustering method is best to reduced energy[5].

2. *Prevantion from vampire attack:* A Vampire attack on the composition and transmission of a message are consumed more energy than the honest node change the packet node header. This problem is solved by no-backtracking algorithms and measuring the strength of the attack by the ratio of network energy used in the benign case to the energy used in the malicious case. Safety from Vampire attacks implies this ratio is equal to 1.

3. Per-node energy usage under attacks: the carousel attack causes excessive energy usage for a few nodes, since only nodes along a shorter path are affected. In contrast, the stretch attack shows more uniform energy consumption for all nodes in the network, since longest route, causing more nodes to process the packet. The carousel attack can be prevented entirely by having forwarding nodes check source routes for loops but this adds extra forwarding logic and thus more overhead. When a loop is detected, the source route could be corrected and the packet sent on. A new class of resource consumption attacks that use routing protocols to permanently disable ad hoc wireless sensor networks by depleting nodes' battery power. These attacks do not depend on particular protocols or implementations, but rather expose vulnerabilities in a number of popular protocol classes. Depending on the location of the adversary, network energy expenditure during the forwarding phase increased.[2]

To identify malicious node, we require the detection to be performed by a public auditor. When a malicious node is identified, the auditor should be able to construct a publicly verifiable proof of the misbehavior of that node. The construction of such a proof should be privacy preserving.[4]

Radio jammer provides security to WSN. Jammer is a intelligent programmable device which disturb to the original waves.

CONCLUSION

Survey based on WSN, APEA (accountable, privacy-preserving and efficient authention) is efficient authentication framework, which achieves security, privacy, accountability and high efficiency without the help of any trusted third party for wireless access networks. Clustering based wireless sensor network will solve the problem of security and privacy issues. Grid, hierarchy, linked cluster, double hierarchy cluster are different clustering methods.

The clustering with use of jammer will be providing more security to WSN.

REFERENCES

[1] Daojing He, Sammy Chan and Mohsen Guizani, "An Accountable, Privacy-preserving and Efficient Authentication Framework for Wireless Access Networks", IEEE journal Transactions on Vehicular Technology, DOI 10.1109/TVT.2015.2406671, 2015.

[2] Tao Shu and Marwan Krunz, "Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 14, NO. 4, pp-, 813-828, April 2015.

[3] Avik Sengupta and Ravi Tandon, "Fundamental Limits of Caching With Secure Delivery", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 2,pp-355-370, February 2015.

[4] and T. Charles Clancy, Senior Member, IEEE

[5] Truc Thanh Tran and Hyung Yun Kong, "CSI-Secured Orthogonal Jamming Method for Wireless Physical Layer Security", IEEE COMMUNICATIONS LETTERS, VOL. 18, NO. 5, pp-841-844, MAY 2014.

[6] SHI LeyP, FU Wenjing, JIA Cong, LIU Xinl and IA Chunfu, "A Sensor Anonymity Enhancement Scheme Based on Pseudonym for Clustered Wireless Sensor Network", IEEE Journal, China Communications· September 2014.

[7] Perumalraja Rengaraju, Chung-Horng Lung, Member, and Anand Srinivasan, "QoS-Aware Distributed Security Architecture for 4G Multihop Wireless Networks", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 63, NO. 6, pp-2886-2900, July 2014.

[8] Shih-Chang Lin and Chih-Yu Wen, "Device-Based Asynchronous Ranging and Node Identification for Wireless Sensor Networks ", IEEE SENSORS JOURNAL, VOL. 14, NO. 10, pp-3648-3661, October 2014.

[9] Yi-Shing Liou, Rung-Hung Gau and Chung-Ju Chang, "Dynamically Tuning Aggression Levels for Capacity-Region-Aware Medium Access Control in Wireless Networks", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 13, NO. 4, pp-1766-1778, April 2014.

[10] Eugene Y. Vasserman and Nicholas Hopper, "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 2, pp-318-332, February 2013.

[11] D. J. Dechene, A. El Jardali, M. Luccini, and A. Sauer, "A Survey of Clustering Algorithms for Wireless Sensor Networks", IEEE, 2010.