Security Improvement of Dropper Elimination Scheme for IoT Based Wireless Networks

Ms.M.sudha
Department of Computer Science, IFET College of Engineering, Villupuram,

Mr.D. Saravanan
Senior Assistant Professor, Department of computer Science, IFET College of Engineering, Villupuram,

Mrs.S.Usharani
Associate Professor, Department of Computer Science, IFET College of` Engineering, Villupuram,

Abstract*—Eliminate the eavesdropper collusion occurredby the two or more devices communicating via optimal relay with centralized router using IOT network. The overall delay is reduced with increase in throughput.This paper studies the important of Received signal strength of wireless communication under eavesdropper collusion where detecting the malicious node. To provide knowledge about the security improvement in wireless communication network by using RSS algorithm.*

Keywords*—Security,Internet of Things, Eavesdroppercollusion, Received Signal Strength (RSS)*

I. Introduction

The Internet of Things (IOT) is a two or more devices connecting through network. Physical device are electronics, sensors, actuator etc. Object participant in limited transmission range in network.so that each objecthas very low battery constraints. In this network connectivity to enable these collections of object and data interchange. In network obtain the various attacks such as passive attack and active attack. It is representing by the malicious node.

II. Related Work

Hu and Evans Directional antennas used to developa protocol for prevent the wormhole attack. Directional antennas are used to detect the angle of arrival of a signal. In this protocol, two nodes communicate knowing that one node receiving messages from one angle and the other node receiving from the opposite angle. This protocol fails only if the attacker intentionally placed wormholes living between two directional antennas. Another localization scheme known as the synchronize system which is involves the work done by **Nagpal, Shrobeand Bachrach**at Massachusetts Institute ofTechnology (MIT). It uses a subset of GPS nodes to provide nodes without GPS a sense of relative location. This is achieved using algorithms: The gradient which measures a GPS node's hop count from a point in a network, which determines the way GPS nodes spread information of its location to nodes without GPS. . A fault in using this scheme is that wormholes can interrupt hop counts inside a network. Hop count mention the distance of source node. Therefore, any system subsequent this scheme is extracted defenceless under wormhole attacks then avoids the wormhole attack.

El Kaissiet.al obstacles hinder the successfulplacement of sensor networks. In accumulation to the limited resources issue, security is a major concern especially for applications such as home security monitoring, battle field, and military applications. This paper presents a defence mechanism against wormhole attacks in wireless sensor networks. Specifically, proposed by the simple protocol tree.

Y. C. Hu et.al considered packet leashes– geographicand It is not easy to determine the packet. In temporal leashes, extremely correct globally synchronized clocks are used to destine the propagation time of packets that could be hard to obtain particularly in low-cost sensor hardware. Even available of timing

analysis may not be able to detect physical layer wormhole attacks or cut-through.

II. System Model

A. *Reputation module*

- The reputation module is responsible for managing the details about participate node in network.
- Each and every node maintains the adjacent node of information.
- IOT network adopt a decentralized approach in which every node maintains of other node details. It is used for identify the intermediate node for data transmission in which way to passing the message.

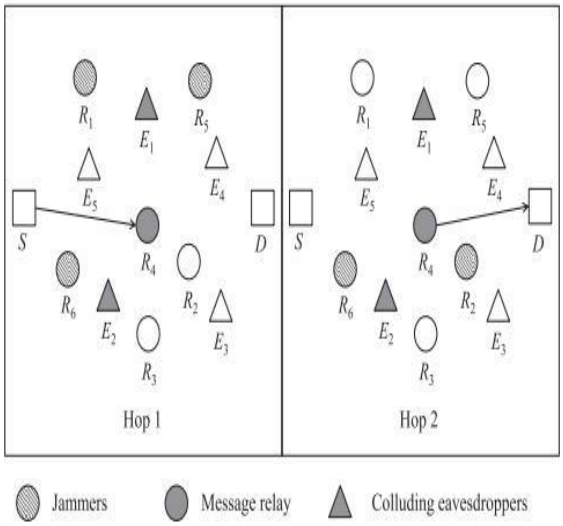
B.DSR-based Route Discovery

- In DSR, source node check the route path exist or not in cache. If it does not exist, source node(S) sends the RREQ message to all other intermediate node in network.
- RREQ message obtain the source and destination ID, and the time-to-live for request 2.
- If any intermediate nodes receive this RREQ message, identify the source node and then rebroadcasts the RREP message while decreasing the time to live value reduce by one.

C.*The audit module*

- The audit module is responsible for detecting misbehaving nodes along entire paths from a source to a destination
- Contrary to previously proposed misbehavior detection mechanisms, the audit module operates on an end-to-end basis, thus allowing the concurrent behavior evaluation of all nodes along a particular path
- Moreover, this module is designed to operate in a resource-efficient manner, by eliminating the need for energy-expensive overhearing techniques

III.SYSTEM ARCHITECTURE



In this diagram consider the two hop wireless network,where a message is first transmitted from its source to intermediate relay(s) and then forwarded by the relay(s) to its destination, serves as an important network model widely adopted in the literature. Actually, understanding the performance of such basic networks lays the foundation for the performance study of general wireless networks. In two hop of employs are S,R,E where R represent for the relay node based on the opportunistic relaying scheme,S represent for the source and E represent for the eavesdroppers that try to intercept the message.

A. *Opportunistic Relaying*

The transmission is conducted in two hops with the help of the opportunistic relaying scheme, where a relay with the largest announces itself as the message relay in a distributed manner before the transmission. We assume that only one transmission, including the relay selection, can be conducted in one time slot. To ensure the secure transmission, we consider the cooperative jamming, a typical physical layer security method where helper jammers generate artificial noise to counteract the eavesdroppers.

B. *Eavesdropper Scenarios*

- **Non-colluding case**: each eavesdropperworks independently and decodes the message from the sensing node solely based on its available observations
- **M-colluding case**: any eavesdroppers (say,as illustrated in Fig) can combine their available observations to decode the message from the sensing node

- These colluding eavesdropper can be treated as a super eavesdropper with M antennas, whose SIR is given by the aggregate SIR of all antennas.

IV.EXISTING SYSTEM

A. *Introduction*

- Conventionally, wireless communication protocols usually use secret keys of various kinds to ensure encryption capability such that, even if an eavesdropper captures packets, it cannot decrypt **them without thekey**
- However, as the computing capability of eavesdroppers continues to advance (e.g., byadopting the quantum computing technology, these encryption protocols may face increasingly high risk of being broken in the future

B.ProblemDefination

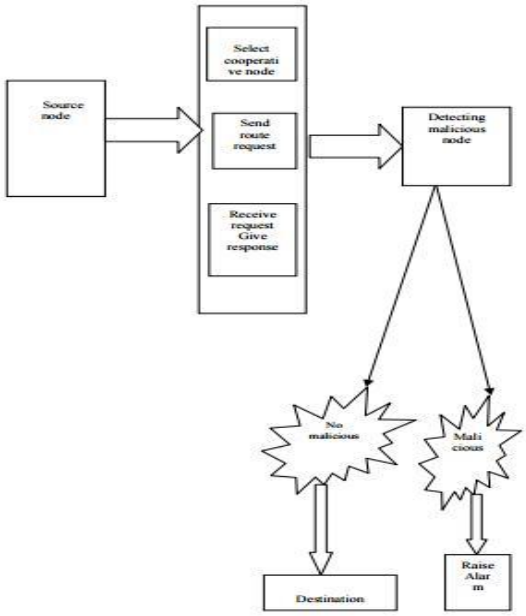
- we adopt the secrecy outage probability (SOP) to characterize the secrecy outage performance, which is defined as the probability that the received packet data ratio of at least one of the eavesdroppers is above some threshold for a transmission
- To design a secure IOT system, the designers first need to specify a maximum allowable SOP for the system

C.Disadvantages of Existing System

- The secret key management and distribution are costly and complex to be implemented in decentralized wireless IOT data collection, where nodes are highly constrained in terms of the computing capability
- Need for secret key management/distribution and an everlasting security guarantee

V.METHODOLOGY

- In this paper, we select any node as the source node from participant node in a network. To use cache block list, we select all intermediate node for message passing via that node
- Route request send to all intermediate node by source node. If it is get the route request packet then give response for that route request packet
- When the source node received the route response packet then its move to RSS algorithm, which is used to detecting the malicious node .which is split the node into two type
- One is no malicious node and another one is malicious node. If the node is No malicious type which is move to destination then raise alarm for detecting malicious node
- In this methodology used by RSS algorithm (Received Signal Strength) capture the malicious by the signal strength of intermediate node. It is also used for optimal relay node via transmitting message from source to destination node with security



VI. PROPOSING SYSTEM

- The Received signal Strength(RSS) is presented that effectively detects the malicious nodes that attempt to launch grey hole/collaborative black hole attacks
- The address of an adjacent node is used as bait destination address to bait malicious nodes to send a reply RREP message, and malicious nodes are detected using a reverse tracing technique

A. Advantage of Proposed System

- In this setting, it is assumed that when a significant drop occurs in the packet delivery ratio, an alarm is sent by the destination node back to the source node to trigger the detection mechanism again
- This function assists in sending the bait address to entice the malicious nodes and to utilize the reverse tracing program of the CBDS to detect the exact addresses of malicious nodes.

VII.CONCLUSION

An eavesdropper is one of the prominent attacks that are formed by malicious colluding node. The section and evasion of such eavesdropper in an IOT network is still considered a challenging task. By using in this concept in simulation one can avoid the eavesdropper collusion and secure transmission from source to destination in IOT network.Now total there will be three simulations as result of which we will show result in the form of comparison between all the three scenarios using the below performance matrices.

1. Throughput
2. Average End to End Delay
3. Packet Delivery Ratio

VIII. REFERENCE

[1]. C.Perkins, IOT networking, Addison-Wesley, 2000.

[2]. J. Sun, Mobile IOT networking: an essential technology for pervasive computing. Proceedings of International Conferences on Infotech&Infonet, Beijing, China, C: p. 316–321.

[3]. M. Bansal, R. Rajput, and G. Gupta, Mobile IOT networking (MANET): routing protocol performance issues and evaluation considerations.Mobile IOT Network (MANET) Working Group, IETF (1998).

[4]. H. Yang, H. Luo, F. Ye, S. Lu, et. al., Security in mobile IOT networks: challenges and solutions. IEEE Wireless Communications,2004. 11(1): p. 38-47.

[5]. M. Lasermann, Characterizing MANET topologies and analyzing their impact on routing protocols. Diploma Thesis,Stuttgart University, Germany, 2002.

[6]. C.Perkins and P. Bhagwat. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. In Proceedings of SIGCOMM '94 Conference on Communications, Architectures, Protocols, and Applications,(London, UK, Sept. 1994), p. 234-244.

[7]. C.Adjih, A.Laouiti, P.Minet, et. al. Optimized link state routing protocol. Work in Progress, IETFdraft, MANET Working Group,INRIARocquencourt, France, 2003.

[8]. C .Perkins and E. Royer. IOT on-demand distance vector routing. In Workshop on Mobile Computing and Systems Applications,1999.

[9]. D. Johnson and D. Maltz, Dynamic Source Routing in IOT wireless networks. In Mobile computing, T. Imielinski and H. Korth, Eds. Kluwer Academic Publishers, 1996: Ch. 5, p. 153-181.

[10]. A. Mukherjee, S. Fakoorian, J. Huang, and A. Swindlehurst, ―Principles of physical layer security in multiuser wireless networks: Asurvey,‖*IEEECommun. Surveys Tuts*, vol. 16, no. 3, pp. 1550–1573, 2014.

[11]. X. He and A. Yener, ―Two-hop secure communication using an untrusted relay,‖ *EURASIP J. Wireless Commun. Netw.*, vol. 2009, pp.1–13, May 2009

[12]. G. Geraci, S. Singh, J. Andrews, J. Yuan, and I. Collings, ―Secrecyrates in broadcast channels with confidential messages and external eavesdroppers,‖ *IEEE Trans. Wireless Commun.*, vol. 13, no. 5, pp.2931–2943, May 2014.

[13]. M Khandakerand K.-K. Wong, ―Masked beam forming in the presence of energy-harvesting eavesdroppers,‖ *IEEE Trans.Inf. Forensics Security*,vol. 10, no. 1, pp. 40–54,2015.

[14] C. Wang, H. Wang, D. Ng, X. Xia, and C. Liu, ―Joint beam formingand power allocation for secrecy in peer-to-peer relay networks,‖*IEEE Trans. Wireless Commun.*, vol. 14, no. 6, pp. 3280–3293, Jun. 2015.

[15] S. Vasudevan, S. Adams, D.Goeckel, Z. Ding, D. Towsley, and K.Leung, ―Multi-user diversity for secrecy in wireless networks,‖ in *Proc.IEEE ITA*, Jan. 2010, pp. 1–9.

[16] J. Zhang, L. Fu, and X. Wang, ―Asymptotic analysis on secrecy capacity in large-scale wireless networks,‖ *IEEE/ACM Trans.Netw.*, vol. 22, no. 1, pp. 66–79, Feb. 2014.

[17] M. Mirmohseni and P. Papadimitratos, ―Scaling laws for secrecy capacity in cooperative wireless networks,‖ in *Proc. IEEEINFOCOM*, Apr. 2014, pp. 1527–1535.

[18] T.Yang, G. Mao, and W. Zhang, ―Connectivity of wireless information theoretic secure networks,‖ in *Proc IEEE GLOBECOM*, Dec.2014, pp. 317–323.