ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

Security Management for Wireless Sensor Network under Eavesdropper Attack

M.Ramya[1], M.Ramani[2]

PG Student [ECE], Dept. of ECE, Sri Manakula Vinayagar Engineering College, Puducherry, India[1]

Assistant Professor, Dept. of ECE, Sri Manakula Vinayagar Engineering College, Puducherry, India[2]

ABSTRACT: Nowadays, wireless sensor networks (WSN) connect the infrastructure of physical entities tightly with the information network. Wireless networks normally has the security threats like eavesdropper attack, as the wireless transmission medium is more affected by the security attacks than those of the guided transmission medium. Understanding the security performance of wireless networks will lay the foundation for security management of the Internet of things (IoT). This paper examines the important secrecy outage performance of wireless communications in the presence of the eavesdropper attack. Based on the link stability based received signal strength on IoT network, the security probability is increased by adapting the outage probability value of the intermediate node or random forwarder. Based on the threshold and outage probability based packet loss ratio, the percentage of droppers are eliminated in the network. The algorithm is implemented using network simulator-2.

KEYWORDS: Eavesdropper collusion, Security probability, Packet loss ratio.

I. INTRODUCTION

The technological advances in the field of communication, wireless communication have become existing everywhere due to the freedom, cost savings, nature of distributed capabilities which they offer. Sensor network have emerged as the next signal of wireless technology which enables the distributed measurements across the large physical environmental systems. In such networks, the transmission within the users can be easily determined by an eavesdropper for interception due to the broadcast nature of wireless transmission medium, making the transmission more vulnerable to dropper attacks. In order to achieve the secured or confidential transmission of information, existing systems adopt the cryptographic techniques to prevent an eavesdropper from recording the data transmission between legitimate or the accepted users [1]. The original data is first encrypted at source node by using an encryption algorithm along with a secret key that is shared with destination node alone. Next, the encrypted plaintext or cipher text is transmitted to destination that will decrypt the received cipher text with the secret key. Likewise, even if an attacker intends to hear the cipher text transmission, it is difficult to translate the plaintext by the eavesdropper from its intercepted cipher text without the key. It is understood that the cipher text transmission is not more secure, because the cipher text can be decrypted by an eavesdropping attacker with the exhaustive key search. So the physical-layer security is appearing as an alternative way to protect the wireless communications against eavesdropping attacks.

Physical-layer security work was done by Wyner in [3], where a discrete memory less channel was determined for secure communications in the presence of an eavesdropper. It was proved that the confidential data transmission can be achieved if the channel capacity of the main link is more than that of the wire link.Next, in [4], the Wyner's results were expanded from the memory less wire channel to the Gaussian wire channel, where a secrecy capacity was developed and shown as the difference between the channel capacity of the main link and that of the wire link. If the secrecy capacity is below zero, the transmission from source to destination becomes insecure and the eavesdropper or the attacker would succeed in intercepting the source event. So in order to improve the attacks, it is of importance to reduce the probability of occurrence of an intercept probability through increasing the secrecy capacity.
As the extensive works concentrated in increasing the secrecy capacity of wireless communications by considering the multiple antennas [5] .Specifically, the multiple-input multiple-output channel was analysed in [7] to increase the wireless secrecy capacity in fading environments. In [8], the co-operative relays were examined for improving the physical-layer security in terms of the secrecy performance. A hybrid cooperative beam forming and jamming approach was investigated in [9] to enhance the secrecy capacity, where partial relay nodes are accepted to assist the source

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

transmission to the allowed destination with the aid of beam forming, while the another remaining relay nodes are used to transmit noise for avoiding the eavesdropper.

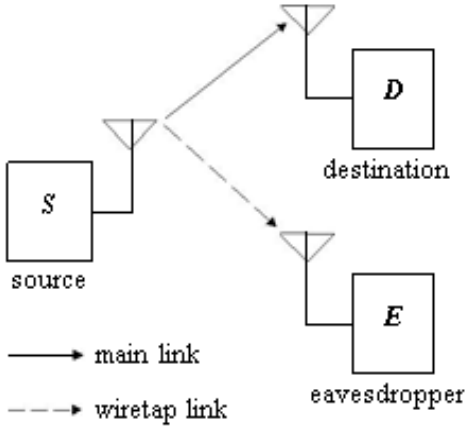

Fig. 1. A wireless communications scenario in the presence of an eavesdropping attack

The security is still guaranteed even if the eavesdroppers have unbounded computating capability. The core idea of PLS is utilizing the inherent randomness and difference of wireless channels to keep the confidential message secure from eavesdropper, regardless of the attacker.The transmit power of many IOT objects like sensors and mobile phones is low, which limits the coverage range for the secure communication. The authors in [2] have optimized the power allocation and transmission region for the decode and forward relay network under the secrecy outage constraint. It is assume that the system designer knows the instantaneous channel state information or at least the channel distribution information of eavesdropping attacker. This is an impractical assumption since most eavesdroppers are passive attackers, that is, they only listen without transmitting any signals. Moreover, the potential eavesdroppers in the network may be some unusual accepted devices that belongs to different systems. Hence, the exact no and locations of these attackers are difficult to be determined.

II .APPROACH AND CONTRIBUTIONS

In this paper, we examine the secure transmission from a source (e.g., surveillance camera) to a destination (e.g., controller) in the IoT with unknown eavesdroppers. Besides the source and the destination, an intermediate or relay node has to retransmit the secret message. To avoid the using of maximum ratio combining at any eavesdropper, the widely-used randomize-and-forward (RF) is used. For the RF protocol, the source and the intermediate node use various codes to transmit the same secret message. By optimizing the power allocation between the source and the relay as well as the code rate for each hop of the relay transmission, we increase the secrecy under the outage-probability constraint.

First, we concentrate on the antenna system where all the devices including eavesdroppers are equipped with the single antenna. Here it is assumed that the locations of droppers change independently from hop to hop, we derive an equation for the secrecy outage probability of the two-hop transmission, which is shown to be the upper bound of the outage probability when the locations of droppers remain unchanged. Following this expression, we formulate a secrecy maximization problem with the outage- probability constraint. The optimal design for code and power allocation between the source and relay are derived. By studying the performance of the optimal scheme in some special cases, we obtain several insights concerning the system parameter setting. To further analyse the secrecy performance of relay transmission, we then consider the above results to a generic system where the relay and attackers are equipped with more antennas.

This model describes a kind of relay transmission in heterogeneous networks, consisting of two kinds of nodes: Low-

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

end and High-end sensors. The source and the destination are Low-end sensors with single antenna and another one with multiple antennas serves as a relay. In practice, here the noise is not suitable for network applications since it requires high consumption of energy as well as causes interference to nearby sensor nodes [6].Thus, in this work we only consider the beam forming as our transmit plan without providing artificial noise. The expression for the secrecy outage probability is derived, based on which a similar secrecy rate maximization problem is formulated. Through this optimizing method, we obtain the optimal solution which is a generalization of the solution derived for the antenna system.

III. SYSTEM MODEL

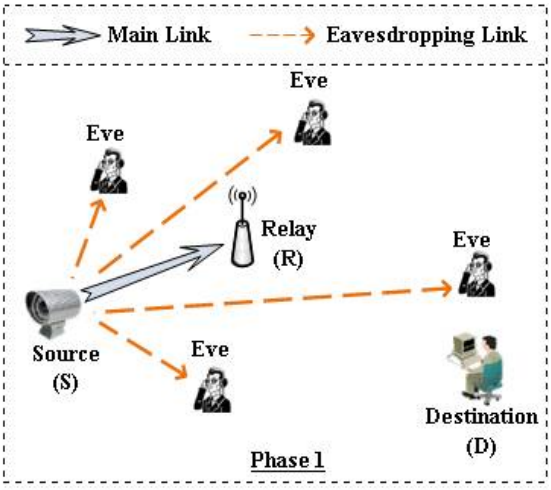

Fig. 2. The source node S is transmitting confidential message to the destination node D with the help of a relay R

The system model is illustrated in Fig. 2 for the application to choose two rates to construct a wire code: the rate of transmitted Packets and the rate of confidential or the secure message. For the code of phase i (where i=1,2) denote the rates of transmitted Packets and the confidential message as Rt and Rs respectively. Here the source node S is transmitting secure message to the destination node D with the help of a selected nearby neighbor node or the relay. Randomly distributed eavesdroppers or the attackers are trying to interpret the message.

Note that in the relay network, although the code rates for different phases can be changing, the rate of the confidential message should not change [2].The source node S Rs,1 = Rs,2 = Rs. The rate difference Re,i = Rt,I -Rs, (e.g., surveillance camera) needs to transmit the collected data to the destination node D (e.g., controller) for the safety management. A intermediate node or the relay node is employed to forward the message. Thus, the whole transmission is composed of two phases (hops),as shown in Fig. 2

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

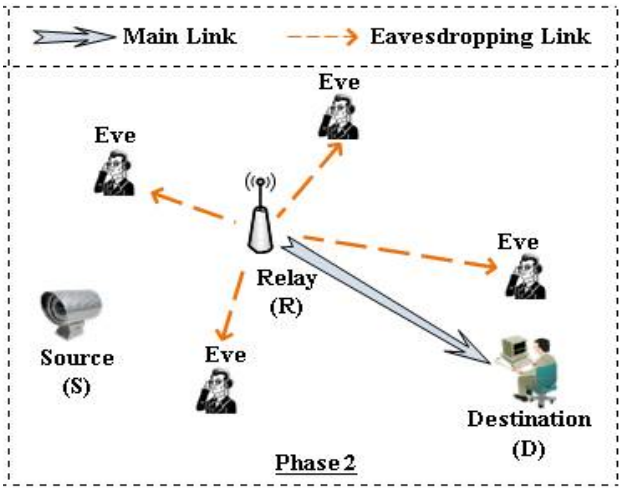

Fig.3.Relay node (R) is transmitting message to destination node

It is supposed that the intermediate node has already been selected before communications, and the discussion on relay selection is beyond the scope of this paper. In the network, there also exist non- colluding eavesdroppers who operates individually to interpret the secure the message without information sharing between them. As given in Fig. 3, the main link is defined as the link between the accepted devices whiles the attacker link is defined as the link between the allowed transmitter and the eavesdropper. Generally, the locations and channel states of these eavesdroppers are unknown since eavesdroppers only listen without transmitting any signal. we assume that the spatial distributions of eavesdroppers change independently from one transmit phase to another and the location set of eavesdroppers in phase i is modeled as packet delivery ratio with the same density. Although they only presented the proofs for single-antenna system, it is not difficult to see that the conclusion also holds for the multi-antenna system.

In the proposed RSS approach, there are three steps to achieve the probabilistic prediction coefficient in order to estimate the link stability for reliable data delivery in the entire network.
The three steps incorporated in the distributed approach for determining the link stability are

a) Estimation of neighborhood stability based on Energy
b) Estimation of neighbor stability based on link loss
c) Manipulation of lifetime of the mobile relay node

A. ESTIMATION OF THE NEIGHBOURHOOD RELAY STABILITY BASED ON ENERGY

Equation (1) represents the estimation of the neighborhood relay stability based on energy. Let Et denotes the total energy of a mobile node 'i' ,$\boldsymbol{R_e(i)}$ and $\boldsymbol{P_r(i)}$denotes the residual energy and the number of packets relayed by the node 'i'. Let$\boldsymbol{E_r}$be the maximum energy required for transmitting a single packet and $E_u(i)$ be the energy utilized by a nodes present in the path between source and destination, then

$$Eu(i) = (Re(i)-Er\times Pr(i))/Et \quad , \quad (1)$$

The energy information in this multicast environment is recorded in the table containing three fields viz.,

i) Node ID
ii) Multicast GroupID
iii) Timestamp

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

B. ESTIMATION OF NEIGHBOR RELAY STABILITY BASED ON LINK LOSS

The equation (2) represents estimation of neighbor relay stability based on link loss is given as,

$$LE = (N_R P / N_S P) \times 100 \quad , \quad (2)$$

Where LE is the link Estimate
N_R = No. of Retransmit Packet,
N_S = Total no of packet send.
If LE value is inversely propose to link quality.

C. MANIPULATION OF LIFETIME OF RELAY

The equation (3) represents the manipulation of lifetime of relay is given as,

$$E = n_t * t + n_r * r + s \quad , \quad (3)$$

Each 5 nanosecond E value is calculated as FE= IE-E. Here if FE=0 then node become died.
Where IE is Initial energy and FE is final energy.

Here t is the energy consumption for transmitting one packet, nt the number of sent packets, r as the energy consumption for receiving one packet, nr the number of received packets, and s is the energy consumption during the sleep phases. The energy consumption for sending a packet is the product of transmission time and current consumption during packet transmission.

IV.RESULT AND DISCUSSION

The simulation is done in NS2 SOFTWARE. Network Simulator (NS) is a simulation tool targeted at both wired and wireless networking research. It provides substantial support for simulation of routing and multicast protocols over wired and wireless networks. The latest version of NS is 2.26 (NS2).

1. Throughput : Throughput is the rate of successful message delivery over a communication channel. Throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second (p/s or pps).

Fig.4 :Throughput

Fig.4 represents the variation of throughput with change in time in case of eavesdropper attack. If the attackers are increased throughput will be affected. After elimination of attackers the overall throughput was increased.Higher the throughput better is the protocol.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

2. Delay : The delay is defined as the average time taken by a data packet to arrive in the destination. It is the delay caused by route discovery and the queue in data packet transmission.

Fig.5. Delay

Fig.5 shows the variation of end to end delay with respect to time in case of eavesdropper attack. Only the data packets that successfully delivered to destinations will be counted. In existing work, each time the dropped packets should be resend. This will cause the additional packet delay. But in proposed work there is no need to resend the packet. This will result in better delay efficiency.

3. Packet delivery ratio: It is the ratio of packets that are successfully delivered to a destination compared to the number of packets that have been transmitted from source node.

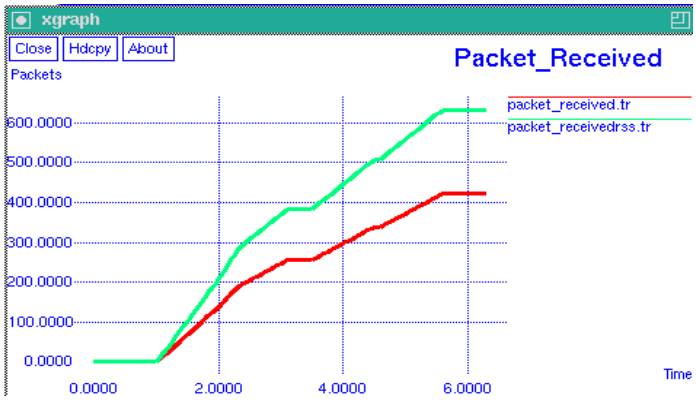

Fig.6 Packet Delivery Ratio

Figure 6 shows the variation of Packet received with time for eavesdropper attack. This illustrates the level of delivered data to the destination. Dropper will cause more drops in conventional system. But in proposed system there is no droppers. However by applying link stability based rss approach, the corresponding PDR value increases further.

4. Link Threshold : Link threshold is the fixed value to determine the secrecy outage probability.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

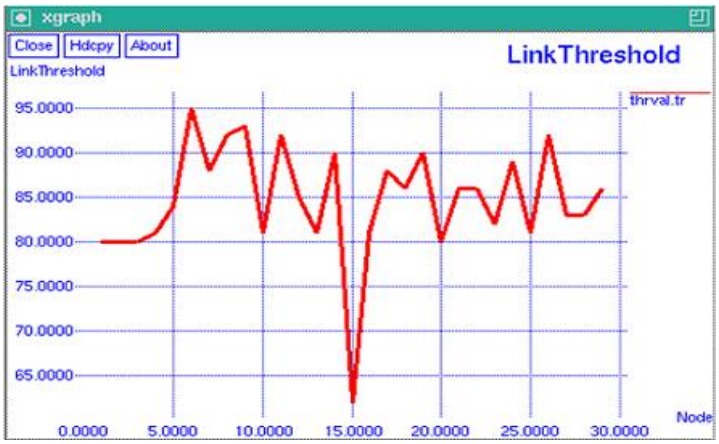

Fig.7 Link Threshold

Fig.7 shows the variation of link threshold with respect to the nodes during the presence of eavesdropping attack.x axis represents the no of users and the y axis represents the drop ratio. Here the threshold is fixed as 65 to eliminate the dropper node. The node with higher drop ratio will be eliminated.

V.CONCLUSION

With the development of the upcoming 5G communication system, the concept of IoT is attracting more and more attention. 5G technologies hold the potential to enable a seamless connection among the various kind of the things. However, heterogeneous environment in 5G systems make the communication vulnerable to eavesdropping attack. In this paper, we studied the secure relay communications in IoT networks against randomly distributed eavesdroppers. We first considered a simple scenario where all the devices including eavesdroppers are equipped with the single antenna. The secrecy outage probability under this scenario was derived, based on which we formulated a secrecy-rate- maximization problem. The optimal power allocation and code word rates were derived. We then studied this optimization problem in a more generic scenario where the relay and eavesdroppers are equipped with multiple antennas. We obtained the expression for the secrecy outage probability which is similar to the expression derived for the single antenna system. Due to the similarity, we directly utilized the previous results to obtain a generalized optimal scheme. By using numerical simulations, we validated the optimality of the proposed scheme and found that the optimal scheme can be replaced by a simple suboptimal one with only a little performance loss. Moreover, it was shown by numerical results that equipping the relay with multiple antennas are always beneficial even if the eavesdropper has the same number of antennas. Finally, by comparing the performance of relay transmission with direct transmission, we found that the appropriate introduction of relay transmission can enhance the secrecy throughput and extend the secure coverage area.

REFERENCES

[1] J. Zheng, D. Simplot-Ryl, C. Bisdikian, and H. T. Mouftah, "The Internet of Things," IEEECommun. Mag., vol. 49, no. 11,pp.30–31,Nov.2011.
[2] T. X. Zheng, H. M. Wang, F. Liu andM. H. Lee, "Outage constrained secrecy throughput maximization for DF relay networks," IEEE Trans. Commun., vol. 63, no. 5, pp. 1741–1755, May 2015.
[3] Z. Su, Q. Xu, H. Zhu, and Y. Wang, "A novel design for content delivery over software defined mobile social networks," IEEE Network, vol. 29, no. 4, pp. 62–67,Jul. 2015.
[4] Z. Su, Q. Xu, and Q. Qi, "Big data in mobile social networks: A QoE- oriented framework," IEEE , vol. 30, no. 1, pp. 52–57, Jan. 2016.
[5] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, andM. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," IEEE Commun. Surv. Tutor., vol. 17, no. 4, pp. 2347–2376, Nov. 2015.
[6] A. Mukherjee, "Physical-layer security in the Internet of Things: Sensing and communication confidentiality under resource constraints," Proc. IEEE, vol. 103, no. 10, pp. 1747–1761, Oct. 2015.
[7] A. Gupta and R. K. Jha, "A survey of 5G network: Architecture and emerging technologies," IEEE Access, vol. 3, pp. 1206–1232, Aug. 2015.
[8] Q. Du, H. Song, Q. Xu, P. Ren, and L. Sun, "Interference-controlled D2D routing aided by knowledge extraction at cellular infrastructure towards ubiquitous CPS," Personal and Ubiquitous Computing, vol. 19, no. 7, pp. 1033–1043, Oct.2015.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

[9] P. Ren, Y. Wang, and Q. Du, "CAD- MAC: A channel-aggregation diver- sity based MAC protocol for spectrum and energy efficient cognitive ad hoc networks," IEEE J. Sel. Areas Commun., vol. 32, no. 2, pp. 237–250, Feb. 2014.
[10] S.L.Keoh, S. S. Kumar, and H. Tschofenig, "Securing the Internet of Things: A standardization perspective," IEEE IoT J., vol. 1, no. 3, pp. 265–275, Jun. 2014.