IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-9, Sept. 2018 E-ISSN: 2347-2693

An Efficient Jamming Node Avoid Secure Routing In Internet of Things

E. Selvi[1*], K. Renuka[2]

[2]Department of Computer Science, Rathinam College of Arts and Science, Coimbatore, Tamil Nadu, India
[2]Department of Computer Science, Rathinam College of Arts and Science,Coimbatore, Tamil Nadu, India

Available online at: www.ijcseonline.org

Accepted: 19/Sept/2018, Published: 30/Sept/2018

***Abstract*—** The shared wireless medium, wireless networks are vulnerable to jamming attacks. These types of attacks can easily be accomplished by an adversary by either bypassing MAC layer protocol or by emitting RF signals**.** The **f**ailure of data transmission in internet of things is due to corruption of packets by jammers. In existing no of defense techniques have been proposed in recent years to deal with these jammer attacks. However, each defense technique is suitable for only a limited network range and consumption energy. The propose jamming detection algorithm based on two problem solving, first one is to improve the energy efficient routing based on power allocation and second one avoids the jamming node using ecliptic curve cryptography to route the secure packet between source to destination. The simulation result shows the better throughput and delay minimization compare with existing routing algorithms.

***Keywords*—** IoT, Wi-Fi Sensor devices, Energy routing, Security, Jamming node, Power allocation

I. Introduction

The Internet of Things (IoT) is the informal term for the interconnection of objects or "things", to the existing Internet infrastructure. These devices, usually small embedded computational devices, will transform our concept of Internet connectivity. By equipping objects such as sensor node, cars, washing machines, in-door air control systems, and even our-selves with Internet capabilities, the way that we will interact with these objects and how these objects will interact with each-other will change extremely. The Wireless Sensor Networks (WSN) will play a key role in the information exchange between embedded devices and the Internet. However, wireless communications are not without obstacles and allow objects to become connected to the Internet, efforts must be taken to ensure reliable communication given any external impacts such as interference or absorption.

The IoT devices do not require an any user interface as what is normally expected when working with connected devices. Somewhat, IoT devices are capable to function and make decisions without human control. The devices may collect data, the data might then be processed by some application and a suitable action could then be executed accordingly to some routing algorithm or self-learned pattern recognition software.

The cyber-physical systems refer to a new generation of integrated computational systems with physical capabilities. Expanding the capabilities of these physical systems and the ability to interact with are the keys for the future of technology developments that have a lot of opportunities and research challenges. The principal goal of Cyber-Physical Systems (CPS) is to monitor some physical process behavior they are a part of (through obtained measurement signals), and make decision and take actions to change its behavior accordingly (through control signals).

In wireless network security is growing as a new dimension for resource constrained devices which will integrate the security features right in to the hardware and software parts of the devices. The security in perspective of software services. The IoT system become prone to different security attack, out of all that, system is more prone to jamming attack.

Security is one of the critical attributes of any communication network. Various attacks have been reported over the past many years. At the present time, with the advances in technology, wireless networks are becoming more affordable and easier to build. Many metropolitan areas deploy public IOTs for people to use freely. Moreover, the prevalence of IOTs as the basic edge access solution to the Internet is rapidly becoming the reality. However, wireless networks are accompanied with an important security flaw; they are much easier to attack than any wired network. Although the shared and easy to access medium is great advantage of wireless networks, but it is one of their greatest weaknesses at the same time. In particular, it makes it extremely easy for an adversary to launch an attack. While the goal of traditional DoS attacks is to overflow the user and the kernel domain buffers to deny service, in wireless networks, however, there are many occasions when launching an attack – such as jamming – can be much easier for an adversary.

Jamming is the radiation of electromagnetic energy in a communication channel which reduces the effective use of the electromagnetic spectrum for legitimate communication. Jamming results in the loss of the link's reliability, increased energy consumption, extended packet delays, and disruption of the end-to-end routes. Jamming may be both malicious with the intention to block communication of an adversary or non-malicious in the form of unintended channel interference. In the context of embedded wireless networks for time-critical and safety critical operation such as in Cyber Physical Systems (ex. medical devices and industrial control networks), it is essential that mechanisms for resilience to jamming are easy and fast to detect ongoing attacking on the communication protocol. Resilience to jamming and its avoidance, collectively termed as anti-jamming, are hard practical problem as the jammer has an unfair advantage in detecting legitimate communication activity due to the broadcast nature of the channel.

The organization of this paper is as follows: Section 2 describes the different type of jamming attacks, existing jamming detection method, and jammer-location identification. In Section 3, we give the details of how to propose jammer localize jammers in networks, path outage probability and link outage probability. Section 4 describes propose secure routing protocols for detection and jamming attacks detection. The experimental result compare with existing method to better result in proposed system are described in Section 5. We conclude of work in Section 6.

II. RELATED WORK

It should be realized that the physical layer technologies needed to reliably resist jamming have not found widespread deployment in commodity wireless devices, such as wireless LANs and sensor networks.

There is different type of jamming attack

- Constant jammer
- Reactive jammer

The above jamming models try to break down the communication between two nodes. While they can achieve a high degree of denial of service, they exhibit (in general) low energy efficiency and high probability of detection. Intelligent jamming on the other hand tries to exploit upper layer protocol vulnerabilities.

The secure transmission based on physical layer security mechanism for transmit strategy adaptation with security protection. Specifically, the existing method cooperative transmission is replaced by a cooperative jamming scheme if either security or QoS constraint is not satisfied [1]. Another method statistical analysis based jamming information [2] detection and minimization of security vulnerability region is on the source-destination node packet sending. The exact and some special closed-form terms for the probability of secrecy rate possibility are obtained for the Rayleigh fading channel. Using this, the influence of the location and the relay power on the effective vulnerability area are analyzed and the best cases minimizing this area are numerically computed.

The single antenna system [3] where all the devices including eavesdroppers are equipped with the single antenna. With the assumption that the locations of eavesdroppers change independently from hop to hop, we derive an expression 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 eavesdroppers remain unchanged. Enhance the physical layer security of the single-input-single-output (SISO) [4] wiretap channel. Differing from the existing works, all the helpers in this UCJ scheme are uncoordinated single-antenna uplink users, and each helper transmits a jamming signal independently to confound the eavesdropper. The intended receiver plays the role of base station in the cellular systems as well as a control center to properly allocate the jamming power of each helper to maximize the secrecy rate. Two cases are addressed in solving the secrecy rate maximization problem, namely, the global channel state information (CSI) case and the partial CSI case.

The enhance the physical layer security of the single-input-single-output (SISO) wiretap channel. Differing from the existing works, all the helpers in this UCJ scheme are uncoordinated single-antenna uplink users, and each helper transmits a jamming signal independently to confound the eavesdropper. The intended receiver plays the role of base station in the cellular systems as well as a control center to properly allocate the jamming power of each helper to maximize the secrecy rate [5]. Two cases are addressed in solving the secrecy rate maximization problem, namely, the global channel state information (CSI) case and the partial CSI case.

The physical layer security in wireless communication networks [6] in which a source (Alice) intends to send a confidential message to a legitimate destination (Bob) with the help of a cooperative jammer (CJ), in the presence of a passive eavesdropper (Eve). Assuming that only statistical channel state information (CSI) of Eve is available, artificial-noise (AN) assisted beam forming and cooperative jamming are designed. The goal is to maximize the secrecy rate, subject to a constraint on secrecy outage probability. Numerical results validate the effectiveness of our scheme.

The existing method joint cooperative beam forming, jamming, and power-allocation scheme [7] to enhance the security of an amplify-and-forward (AF) cooperative relay network in this paper. Different from the existing works assuming that the source node always uses its total power, we show that the secrecy rate is a quasi-concave function of the power of the source node so that allocating its total power may not be optimal. The beam former design and power optimization problem can be solved by a bisection method together with a generalized eigenvalue decomposition, which has a semi-closed form and is computationally very convenient. Important secrecy outage performance of wireless communications under eavesdropper collusion, where the physical layer security is adopted to counteract such attack. Based on the classical Probability Theory, we first conduct analysis on the secrecy outage of the simple non-colluding case in which eavesdroppers do not collude and operate independently. For the secrecy outage analysis of the more hazardous M-colluding scenario [8], where any M eavesdroppers can combine their observations to decode the message, the techniques of Laplace transform, keyhole contour integral, and Cauchy Integral Theorem are jointly adopted to work around the highly cumbersome multifold convolution problem involved in such analysis, such that the related signal-to-interference ratio modeling for all colluding eavesdroppers can be conducted and thus the corresponding secrecy outage probability can be analytically determined.

The typical four-node (source, destination, relay, and eavesdropper) scenario, we derive the optimal power allocation for the DF strategy and find that the RF strategy is always better than the DF to enhance secure connection. In cellular networks, we show that without relay, it is difficult to establish secure connections from the base station to the cell edge users. The effect of relay placement for the cell edge users is demonstrated by simulation.

In this paper cooperative wireless network in the presence of one or more eavesdroppers, and exploit node cooperation for achieving physical (PHY) layer-based security [9]. Two different cooperation schemes are considered. In the first scheme, cooperating nodes retransmit a weighted version of the source signal in a decode-and-forward (DF) fashion. In the second scheme, referred to as cooperative jamming (CJ), while the source is transmitting, cooperating nodes transmit weighted noise to confound the eavesdropper. We investigate two objectives: i) maximization of the achievable secrecy rate subject to a total power constraint and ii) minimization of the total power transmit power under a secrecy rate constraint. For the first design objective, we obtain the exact solution for the DF scheme for the case of a single or multiple eavesdropper, while for the CJ scheme with a single eavesdropper we reduce the multivariate problem to a problem of one variable. For the second design objective, existing work introduces additional constraints in order to reduce the degree of difficulty, thus resulting in suboptimal solutions.

The joint relay and jammer selection in two-way cooperative networks [10], consisting of two sources, a number of intermediate nodes, and one eavesdropper, with the constraints of physical-layer security. Specifically, the proposed algorithms select two or three intermediate nodes to enhance security against the malicious eavesdropper. The first selected node operates in the conventional relay mode and assists the sources to deliver their data to the corresponding destinations using an amplify-and-forward protocol. The second and third nodes are used in different communication phases as jammers in order to create intentional interference upon the malicious eavesdropper.

The relay selection in cooperative networks with secrecy constraints. The proposed scheme enables an opportunistic selection [11] of two relay nodes to increase security against eavesdroppers. The first relay operates as a conventional mode and assists a source to deliver its data to a destination via a decode-and-forward strategy. The second relay is used in order to create intentional interference at the eavesdropper nodes. The proposed selection technique jointly protects the primary destination against interference and eavesdropping and jams the reception of the eavesdropper. Physical-layer security in cooperative wireless networks with multiple relays where both amplify-and-forward (AF) and decode-and-forward (DF) protocols are considered. We propose the AF and DF based optimal relay selection (i.e., AFbORS and DFbORS) [12] schemes to improve the wireless security against eavesdropping attack. For the purpose of comparison, we examine the traditional AFbORS and DFbORS schemes, denoted by T-AFbORS and T-DFbORS, respectively. We also investigate a so-called multiple relay combining (MRC) framework and present the traditional AF and DF based MRC schemes, called T-AFbMRC and T-DFbMRC, where multiple relays participate in forwarding the source signal to destination which then combines its received signals from the multiple relays. We derive closed-form intercept probability expressions of the proposed AFbORS and DFbORS (i.e., P-AFbORS and P-DFbORS) as well as the T-AFbORS, T-DFbORS, T-AFbMRC and T-DFbMRC schemes in the presence of eavesdropping attack.

This can be achieved primarily in two ways: without the need for a secret key by intelligently designing transmit coding strategies, or by exploiting the wireless communication medium to develop secret keys over public channels. The survey begins with an overview of the foundations dating back to the pioneering work of Shannon and Wyner on information-theoretic security [13]. We then describe the evolution of secure transmission strategies from point-to-point channels to multiple-antenna systems, followed by generalizations to multiuser broadcast, multiple-access, interference, and relay networks. Secure downlink transmission from a controller to an actuator, with the help of a cooperative jammer to fight against multiple passive and non-colluding eavesdroppers. In addition to artificial noise aided secrecy beam forming for secure transmission, cooperative jamming (CJ) [14] is explored to further enhance physical layer security. In particular, we provide a secrecy enhancing transmit design to minimize the secrecy outage probability (SOP), subject to a minimum requirement on the secrecy rate. Based on a strict mathematical analysis, we further characterize the impacts of the main channel quality and the minimum secrecy rate on transmit designs.

III. METHODOLOGY

The propose power allocation algorithm average energy saved is defined as the reduction in the average energy consumption of the system nodes when the proposed method is applied with respect to the average energy consumption when system nodes use the shortest path between source and destination. The ECC (Elliptic Curve Cryptography) algorithm is using for encryption and decryption method. It protects all data against malicious modification and information forgery. The optimum routing protocols are such as SAODV routing protocols. Power allocation algorithm based on minimum energy routing in a fading environment in the presence of malicious jammers in a wireless IOT network. The ECC algorithm is used to safe guard from different attacks by building a secure route from source to sink node. The routing protocol suffers from jamming attack. Encryption and decryption have been evaluated in terms of data delivery ratio and level of security.

A. System Model

Here consider an IOT wireless sensor network where the sensor nodes are located arbitrarily in the IOT wireless topology. In addition, malicious jammers are present in the network at arbitrary locations, which try to interfere with the transmission of the wireless nodes by transmitting random signals. The multipath routing different source nodes chooses multi relays nodes and tries to convey its message to the multi destination node. Multi-hop fashion. The relays that the source selects construct a K-hop route between the source and the destination. The K-hop route is determined by a set of K links $N = \{l_1 \ldots\ldots l_k\}$and K + 1 nodes (including source and destination) such that link l_k connects the nodes S_k and D_k.

B. Jammer Attack Model

The set of jammers by J and consider both static jammers and dynamic jammers. In the case of static jammers, each jammer transmits the jamming signal constantly and with a fixed power. Since the jammers are active, we assume that the transmit power and the location of jammers are known to the system nodes; however, the random nature of the multi-path fading in the environment makes the interference created by the jammers at receivers random and a priori unknown. Furthermore, we will see that by using our proposed method, the knowledge of transmit power and location of jammers at the system nodes is not necessary; in fact, the system nodes can measure the received jamming for a long time period and use this estimate of jamming interference for efficient routing. In the case of dynamic jammers, each jammer switches between an “ON” state, when it transmits the jamming signal, and an “OFF” state or sleeping mode randomly and independently from the other jammers. These dynamic jammers are especially useful when the battery life of the jammers is limited and the adversary tries to cover a larger area, as the jammers in sleep mode can save significant energy.

C. Path Outage Probability

To find a minimum energy route between an arbitrary pair of nodes in the network such that the desired average end-to-end probability of outage is guaranteed. Hence, we need to find the set of relay nodes (links) with minimum aggregate power such that the end-to-end probability of outage$p_{out}^{SD} \leq \pi$, π is a predetermined threshold for the average outage probability. Let $p_k$out denote the average outage probability of link $l_k = \langle S_k, D_k \rangle$; the source-destination outage probability in terms of the outage probability of each link is,

$$p_{out}^{SD} = 1 - \prod_{1 \leq k \leq K} (1 - p_{out}^{k}) \qquad (1)$$

The formulation is the end-to-end throughput of the path between the source and destination. Let ρ denote the required end-to-end throughput. Since the throughput of a path is determined by the throughput of its bottleneck link, to minimize transmission energy of the path, it is necessary to achieve an equal throughput over each link of the path. Thus, in our formulation of minimum energy routing, the cost of each link is computed with respect to the required throughput ρ.

D. Link Outage Probability

The outage probability of a link in the presence of the set of jammers$\mathcal{J}$. The outage probability of link l_k given its fading gain $|h_k|^2$and the fading gains between the jammers and the receiver of the link, i.e., $\{|h_{j,k}|^2\}_{j \in \mathcal{J}}$ is,

$$p_{out}^{k} = \mathbb{P}\left\{\frac{P_k |h_k|^2 / d_k^{\alpha}}{N_0 + \sum_{j \in \mathcal{J}} P_j |h_{j,k}|^2 / d_{j,k}^{\alpha}} < \gamma\right\} \qquad (2)$$

Where γ is the required signal-to-interference ratio at the receiver? The value of γ determines the link throughput. Specifically, for a desired throughput of ρ.

IV. Secure Minimum Energy Aware Routing

A. Power Allocation

Power allocation problem as a stochastic optimization problem with the objective to minimize the long-term power consumption of the whole system including all mobile devices. The discontinuous reception mode is considered for mobile devices, that is, during the unscheduled period, the mobile devices can sleep for energy conservation. This energy saving approach is in favor of prolonging the standby time of the energy constrained devices such as sensor nodes devices. Besides, the long-term rate requirements of all users are also considered as constraints in the problem formulation, such that the QoS of all users can be guaranteed.

Jamming attack makes the battery of target devices to drain quickly by disrupting their data transmission and making them retransmit repeatedly. The power control problem, must find the optimal transmission power level for all users on each channel. Modeled as a finite horizon joint power control and user scheduling problem. Also, prove that finding an optimal solution is NP-hard. The formulate the problem by exploiting techniques from Dynamic Programming (DP). The DP formulation allows us to show that the joint power control and user scheduling is a decomposable problem. That is, at each optimization step It can sequentially solve the power control and the user scheduling problems. It shows that, under some conditions, it is possible to identify the optimal power control policy, i.e., conservative, exploratory or aggressive. To avoid the curse of dimensionality of the DP approach, it exploits state aggregation techniques to propose an approximated solution and study its complexity.

B. Secure Routing algorithm

ECC is the most efficient public key encryption method based on the concept of elliptic curve which is used for enhanced cryptographic key. Generally, ECC is used to compare with the public key encryption methods like RSA and Diffie Hellman key exchange problem. ECC helps to provide greatest security with low power computing devices. Some public key encryption methods like RSA, D-H key exchange and Digital Signature Algorithm (DSA) are very suitable for high power computation but when we go for IoT or cloud computing then there is a possibility that low power computing devices will not support such types of devices.

The Cryptography is an electronic technique that is used to protect valuable data over transmission. Mainly cryptography is science to provide security to information. To protect our data by using different authentication scheme is the main objective of cryptography. When authentication of data is main consider that should be less cost than the value of original information. It is like RSA public key cryptography. The security strength of ECC depends on the difficulty of Elliptic Curve Discrete Logarithm Problem (ECDLP). ECC adopts scalar multiplication, which includes point doubling and adding operation which is computationally more efficient than RSA exponentiation. The complexity of ECC puts the attacker in difficulty to understand the ECC and to break the security key. The security level given by RSA with 1024-bit key can be achieved with 160 bits key by ECC. Hence it is well suited for resource constraint devices like smart cards, mobile devices, etc. It is also not an easy task to choose appropriate elliptic curve. ECC standardization is crucial for achieving practical and efficient implementation. National Institute of Standards and Technology (NIST) provides specification for ECC which are considered safe for the use in cryptographic application. Two main terms that is used for the cryptography technique are Encryption and Decryption. Encryption technique is used to send confidential data over communication. The process of encryption requires two things (1) an encryption algorithm and (2) key.

- Key Generation

Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key. Now, we have to select a number within the range of 'n'. Using the following equation, we can generate the public key

$$Q = d * p \qquad (3)$$

d = The random number that we have selected within the range of (1 to n-1). P is the point on the curve. 'Q' is the public key and 'd' is the private key.

- Encryption

Let 'm' be the message that we are sending. To represent this message on the curve. This has in-depth implementation details.

Consider 'm' has the point 'M' on the curve 'E'. Randomly select 'k' from [1 – (n-1)]. Two cipher texts will be generated let it be C1 and C2.

$$C_1 = k * p \qquad (4)$$

$$C_2 = M + k * Q \qquad (5)$$

C_1 and C_2 will be sent.

C. Decryption

To get back the message ‘m’ that was sent,

$$M = C_2 - d * C_1 \qquad (6)$$

M is the original message that have send.

The multipath construction phase is to organize the network into levels according to hop distance from the sink node to a sensor node i.e. by the end of this phase each node will get a ring level which indicates how many hops away from the sink node. The nodes which received the packet will increase their ring number and rebroadcast the packet to their neighbors. In the end, all the nodes in IOT are separated into several levels. Now each sensor node has got its own ring level, then they can send data packets to the sink node. Due to the lack of address in wireless sensor network, send a packet to the destination node directly but broadcast it with the node’s ring level. If the nodes’ ring level is lower than the received packet’s ring level, then broadcast the packet with current node’s ring level again, till the packet arrived at the destination node know that if a sensor node wants to send a data to the destination node, it should broadcast the data with its own ring level. The neighbors around the node will receive the data and compare the received ring level with their own ring level, only the lower nodes can process the data. If the received node is the destination node then process the packet or otherwise rebroadcast the data.

V. Results And Discussion

Here considers a wireless network in which n system nodes and n_j jammers are placed uniformly at random on a $d * d$ square. Here assume that the closest system node is the source and the different system node to the point is the destination.

- Packet Delivery Ratio

Packet delivery ratio is defined as.

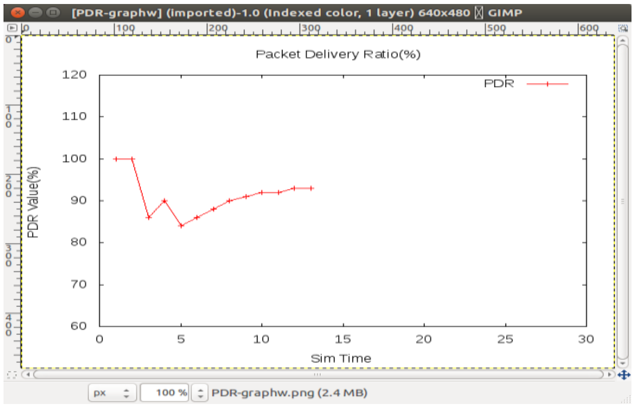

Figure 1. Analysis the packet delivery ratio

Figure 2. $PDR = \frac{\Sigma\, \text{no of packet recived}}{\Sigma\, \text{no of packet send}}$

The ratio of data packets received by the destinations to those generated by the sources. This illustrates the level of delivered data to the destination. Mathematically represented as

- Delay Time

The average time it takes a data packet to reach the destination. This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue. This metric is calculated by subtracting time at which first packet was transmitted by source from time at which first data packet arrived to destination.

$$\text{Packet Delay Time} = S/N$$

Where S is the sum of the time spent to deliver packets for each destination, and N is the number of packets received by the all destination nodes.

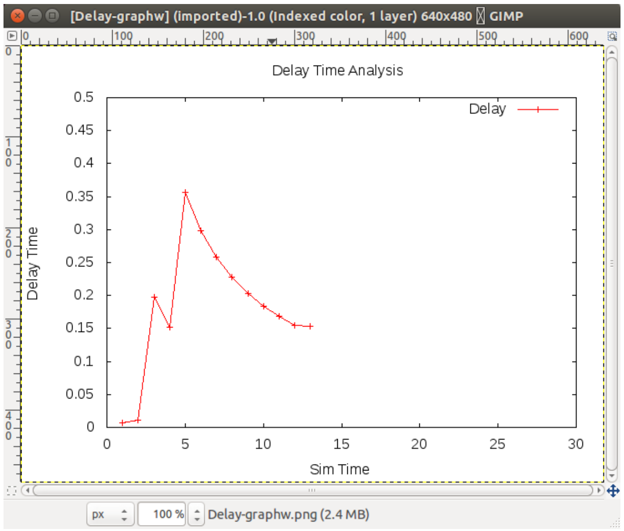

Figure 3. Analysis the end to end delay time

- Average Throughput

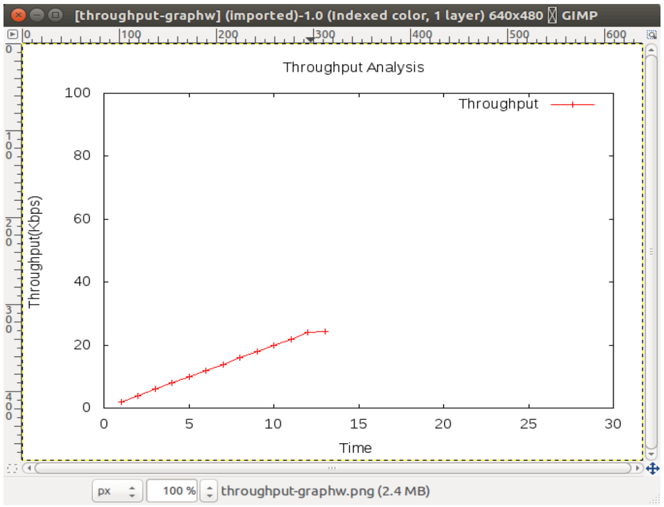

Figure 4. Analysis Throughput analysis

When used in the context of communication networks, such as Ethernet or packet radio, throughput or network throughput is the rate of successful message delivery over a communication channel. Shows the data these messages belong to may be delivered over a physical or logical link or it can pass through a certain network node. Throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot. It is defined as the total number of packets delivered over the total simulation time.

VI. Conclusion

The energy consumption is an important issue in wireless internet of things, minimum energy routing with and without security constraints has received significant attention. Failure of data transmission in sensor networks is due to corruption of packets by jammers. A number of defence techniques have been proposed in recent years to deal with these jammer attacks. However, each defence technique is suitable for only a limited network range and more energy consumption. The propose jamming detection algorithm based on two problem solving, first one is to improve the energy efficient routing based on power allocation and second avoid the jamming node using ecliptic curve cryptography secure routing algorithm. The propose algorithm to measure the signal strength based on reactive reliability and carrier sensing time are able to detect the presence of a jammer node and identify the location of jammer node. The proposed simulation implements in network simulator and compare the existing performance with proposed system.

References

[1] L. Hu, H. Wen, B. Wu, J. Tang, and F. Pan, "Adaptive secure transmission for physical layer security in cooperative wireless networks," IEEE Commun. Lett., vol. 21, no. 3, pp. 524–527, Mar. 2017.

[2] A. Behnad, M. B. Shahbaz, T. J. Willink, and X. Wang, "Statistical analysis and minimization of security vulnerability region in amplify-and-forward cooperative systems," IEEE Trans. Wireless Commun., vol. 16, no. 4, pp. 2534–2547, Apr. 2017.

[3] Q. Xu, P. Ren, H. Song, and Q. Du, "Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations," IEEE Access, vol. 4, pp. 2840–2853, 2016

[4] X. Hu, P. Mu, B. Wang, and Z. Li, "On the secrecy rate maximization with uncoordinated cooperative jamming by single-antenna helpers," IEEE Trans. Veh. Technol., vol. 66, no. 5, pp. 4457–4462, May 2017.

[5] P. Mu, X. Hu, B. Wang, and Z. Li, "Secrecy rate maximization with uncoordinated cooperative jamming by single-antenna helpers under secrecy outage probability constraint," IEEE Commun. Lett., vol. 19,no. 12, pp. 2174–2177, Dec. 2015.

[6] L. Hu, B. Wu, J. Tang, F. Pan, and H. Wen, "Outage constrained secrecy rate maximization using artificial-noise aided beamforming and cooperative jamming," in Proc. IEEE ICC, Kuala Lumpur, Malaysia, May 2016, pp. 1–5.

[7] H.-M. Wang, F. Liu, and M. Yang, "Joint cooperative beamforming, jamming, and power allocation to secure AF relay systems," IEEE Trans. Veh. Technol., vol. 64, no. 10, pp. 4893–4898, Oct. 2015.

[8] Y. Zhang, Y. Shen, H. Wang, J. Yong, and X. Jiang, "On secure wireless communications for IoT under eavesdropper collusion," IEEE Trans. Autom. Sci. Eng., vol. 13, no. 3, pp. 1281–1293, Jul. 2016.

[9] J. Mo, M. Tao, and Y. Liu, "Relay placement for physical layer security: A secure connection perspective," IEEE Commun. Lett., vol. 16, no. 6, pp. 878-881, Jun. 2012.

[10] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," IEEE Trans. Signal Process., vol. 59, no. 10, pp. 4985-4997, Oct. 2011.

[11] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, pp. 310-320, Feb. 2012.

[12] I. Krikidis, J. S. Thompson, and S. Mclaughlin, "Relay selection for secure cooperative networks with jamming," IEEE Trans. Wireless Commun.,vol. 8, no. 10, pp. 5003-5011, Oct. 2009.

[13] Y. Zou, X.Wang, andW. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," IEEE J. Sel. Areas Commun., vol. 31, no. 10, pp. 2099-2111, Oct. 2013.

[14] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," IEEE Commun. Surveys Tuts., vol. 16, no. 3, pp. 1550-1573, Aug. 2014.

[15] Y. Zhang, Y. Shen, H. Wang, J. Yong, and X. Jiang, "On secure wireless communications for IoT under eavesdropper collusion," IEEE Trans. Autom. Sci. Eng., vol. PP, no. 99, pp. 1-13, Dec. 2015.

Author's Biography

Ms.E.SELVI has received her MSc degree in Software Systems from Sree Saraswathi Thyagaraja College, Pollachi affiliated Bharathiar University, Coimbatore, in 2011 and Pursuing M.Phil degree in Computer Science from Rathinam College of Arts and Science, Coimbatore affiliated Bharathiar University, Coimbatore. She is dedicated tamil poet from the last 10 years and published 5 tamil poem books with ISBN. She is currently writing naval book, name of "PAVAIYIN MAUNAM". She is won many prizes in both school and college level Poem, Debate and Essay competitions.

Mrs.K.RENUKA has received her MSc degree in Computer Science from Bharathiar University, Coimbatore, M.Phil degree in Computer Science from Madurai Kamaraj University and pursuing Ph.D degree in Computer Science from Rathinam College of Arts and Science, Coimbatore affiliated Bharathiar University, Coimbatore. She is dedicated to teaching field from the last 11 years and 2 years of industry Experience. She is interested in computer networks and wireless networks and 7 years of research experience. She is guided 7 M.Phil scholars and currently guiding 1 M.Phil scholar.