IOT BASED ENCRYPTION & ROUTINE MODEL FOR DESIGNING AND IMPLEMENTING WSN NETWORK

Rishi Khare, M.Tech Scholar
Vishal Chauhan, Assistant Professor
Infinity Management & Engineering College, Pathariya Jat, Sagar (M.P)-470228

Abstract - In recent years, the concept of IoT has become particularly popular through some representative applications (e. g., smart electric meter reading, greenhouse monitoring, telemedicine monitoring, and intelligent transportation). Usually, IoT has four major components including sensing, heterogeneous access, information processing, applications and services, and additional components such as security and privacy. We consider a practical WSN application, where all hardware transceivers suffer from impairments. The RF technique is employed by the source and relay nodes to prevent the eavesdroppers from combining the source data received over multiple hops. Moreover, these authorized transmitters can adjust their transmit power to reduce the channel capacity obtained on the eavesdropping links.We proposed three novel path selection methods, namely, SPS protocol, RPS protocol, and BPS protocol to investigate the impact of EH and hardware impairments on the outage performance of multi-hop multi-path cooperative WSNs. Moreover, we derive exactly and asymptotically the outage probabilities of three proposed protocols under the presence of one beacon, multiple eavesdropping attacks. The simulation results verified that the employment of BPS together with multi-hop multi-path schemes can enhance significantly the secure performance of the considered EH and hardware impairment system. In particular, BPS is more robust to hardware impairment than RPS and SPS; thus, it can operate better with device that has a poor hardware quality.
Keywords: Matrix Laboratory (MATLAB), Random path selection (RPS), Shortest path selection (SPS), and Best path selection (BPS). Wireless sensor networks (WSNs).

1 INTRODUCTION

The term, internet of things (IoT) that refers to uniquely identifiable objects, things, and their virtual representations in an internet-like structure, was first proposed in 1998 .In recent years, the concept of IoT has become particularly popular through some representative applications (e. g., smart electric meter reading, greenhouse monitoring, telemedicine monitoring, and intelligent transportation). Usually, IoT has four major components including sensing, heterogeneous access, information processing, applications and services, and additional components such as security and privacy. Nowadays, the IoT as a buzzword is widely known, subsequent industry applications related to the IoT will arise, for example cyber-transportation systems (CTS), cyber-physical systems (CPS), and machine-to-machine (M2M) communications

2 THE PROPOSED IOT ARCHITECTURE FROM A TECHNICAL PERSPECTIVE

It is divided into three layers. The basic layer and their functionalities are summarized as follows:

Perception layer: its main function is to identify objects and gather information. It is formed mainly by sensors and actuators, monitoring stations (such as cell phone, tablet PC smart phone, PDA, etc.), nano nodes, RFID tags and readers/writer

Network layer: it consists of a converged network made up of wired/wireless privately owned networks, Internet, network administration systems, etc. Its main function is to transmit information obtained from the perception layer.

Application layer: it is a set of intelligent solutions that apply the IoT technology to satisfy the needs of the users.

An IoT ecosystem consists of web-enabled smart devices that use embedded processors, sensors and communication hardware to collect, send and act on data they acquire from their environments. IoT devices share the sensor data they collect by connecting to an IoT gateway or other edge device where data is either sent to the cloud to be analyzed or analyzed locally. Sometimes, these devices communicate with other related devices and act on the information they get from

one another. The devices do most of the work without human intervention, although people can interact with the devices -- for instance, to set them up, give them instructions or access the data. The connectivity, networking and communication protocols used with these web-enabled devices largely depend on the specific IoT applications deployed.

Motivated by these observations, this proposes three innovative protocols, namely, the shortest path selection (SPS) protocol, random path selection (RPS) protocol, and best path selection (BPS) protocol.

These will enhance the security of multi-hop multi-path randomize-and-forward (RF) cooperative wireless sensor networks (WSNs) under the presence of eavesdroppers and hardware impairment, wherein the source node and relay nodes are capable of harvesting energy from beacon for data transmission. Furthermore, we derive exact closed-form expressions and the asymptotic outage probability for each protocol under multiple eavesdropping attacks.
The simulation results validate the theoretical results.

We propose path-selection methods such as random path selection (RPS), shortest path selection (SPS), and best path selection (BPS).

- In RPS, the source selects randomly a path to communicate with the destination. In SPS, the path with the lowest number of hops is chosen.
- Next, to obtain the optimal outage performance, the BPS method selects the path that provides the highest end-to end channel capacity.
- We consider a practical WSN application, where all hardware transceivers suffer from impairments.
- The RF technique is employed by the source and relay nodes to prevent the eavesdroppers from combining the source data received over multiple hops. Moreover, these authorized transmitters can adjust their transmit power to reduce the channel capacity obtained on the eavesdropping links.

3 OUTAGE PROBABILITY

It is Indication of quality of communication channels. It is measured by finding the probability that a specific transmission rate is not supported.
Outage probability is defined as the point at which the receiver power value falls below the threshold (where the power value relates to the minimum signal to noise ratio (SNR) within a cellular), one can say that the receiver is out of the range of BS in cellular communications.

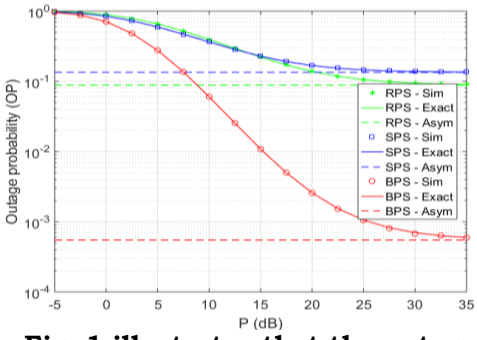

Fig. 1 illustrates that the outage probability value of the BPS protocol is always lower than that of the RPS protocol which further outperforms the SPS protocol. In other words, the BPS protocol achieves the best outage probability performance, further confirming the advantage of proposed best path selection over shortest path selection and random path selection

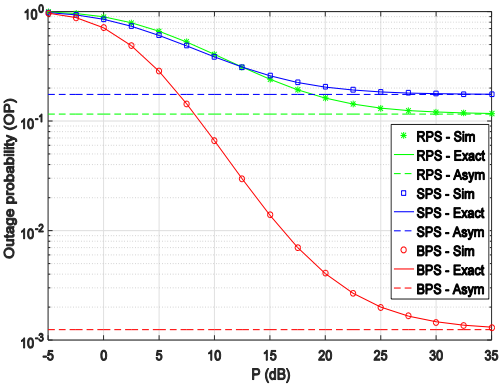

Fig. 2 Outage probability as a function of the transmit power P in dB in the case (a) eavesdroppers do not cooperate and (b) eavesdroppers cooperate together when L = [2, 3, 4], R = 0.5, κ = 0.1, K = 2, (xB, yB) = (0.5, 0.1), (xE, yE) = (0.5, 1), η = 0.1, α = 0

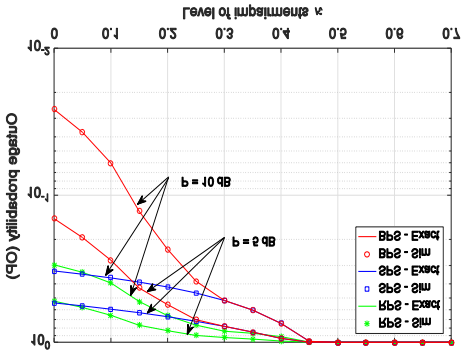

Fig. 3 we investigate the impact of the transmit power of beacon P (dB) on the value of OP in the case that the eavesdroppers do not cooperate and cooperate together by setting L = [2, 3, 4], R = 0.5, κ = 0.1, K = 2, (xB, yB) = (0.5, 0.1), (xE, yE) = (0.5, 1), η = 0.1, α = 0.1.

As shown, there is a good agreement between the theoretical and the simulation results. It is observed that, when P (dB) is small, i.e., P (dB) equal -5dB, OP approaches 1 and when the value of P (dB) increases, OP values decrease. This means that increasing the transmit P can enhance the physical layer security against eavesdropping attacks. Furthermore, comparing the SPS, the RPS, and the BPS protocols,

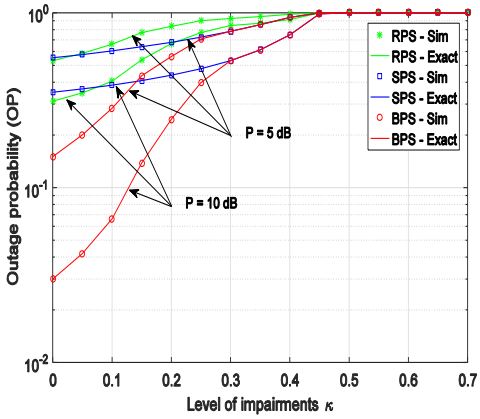

Fig. 4 Outage probability as a function of the level of impairments κ in the case eavesdroppers do not cooperate and eavesdroppers cooperate together when L = [2, 3, 4], R = 0.5, K = 2, (xB, yB) = (0.5, 0.1), (xE, yE) = (0.5, 1), η = 0.1, α = 0.1.

In the outage probability is plotted as a function of xB in the case that the eavesdroppers do not cooperate and cooperate together, when L = [2, 3, 4], R = 0.5, κ = 0.1, K = 2, (xB, yB) = (0.5, 0.1), (xE, yE) = (0.5, 1), η = 0.1, α = 0.1. It is clearly observed that the outage performance of the propose protocols increases to optimal value with increasing xB value is about 0.35 and after that, it decreases.

From this figure, we can determine the position of beacon where the OP reach the optimal value. For example, the OP of BPS and SPS is minimized when xB is about 0.35 or 0.4, the OP of RPS is minimized when is about 0.3 or 0.35.

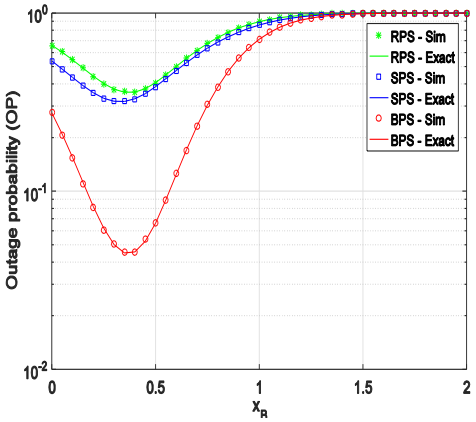

Fig. 5 Outage probability as a function of energy harvesting ratio α in the case (a) eavesdroppers do not cooperate and (b) eavesdroppers cooperate together when L = [2, 3, 4], R = 0.5, κ = 0.1, K = 2, (xB, yB) = (0.5, 0.1), (xE, yE) = (0.5, 1), η = 0.1, α = 0.1.

In Fig, we investigate the impact of yE on the OP in the case that the eavesdroppers do not cooperate and cooperate together, respectively, when L = [2, 3, 4], R = 0.5, κ = 0.1, K = 2, (xB, yB) = (0.5, 0.1), xE = 0.5, η = 0.1, α = 0.1. and xB is set at optimal value 0.35. As shown in Fig. 4a and Fig. 4b, the outage performance increases when the eaves-

4 PARAMETER USED FOR ENCRYPTION

4.1 Correlation Coefficient Analysis

The concept of correlation coefficient is in range between 1.0 (plus or minus one).

A coefficient of +1.0, a "perfect positive correlation," means that can change in the independent item will result in an identical change in the dependent item (e.g., any change in the indicator will result in an identical change in the securities). A coefficient of -1.0, a "perfect negative correlation," means that any change in the independent item will result

in an identical change in the dependent item, but the any change will be in the opposite direction. A coefficient of 0 means there is no relationship between the two items and that any change in the independent item will have no effect in the dependent item.

4.2 Entropy

Entropy is essentially randomness or unpredictability of something in Cryptography, this randomness must be supplied in the plaintext message to remove the structure of the plaintext message.

In some cases a malicious attacker can guess some bits of entropy from the output of a random number generator, and there is need to ensure entropy by adding some elements that the attacker was not privy to

5 RESULTS ON MATLAB

Fig. 6 IOT image encryption script

Fig. 7 Input Image for Encryption

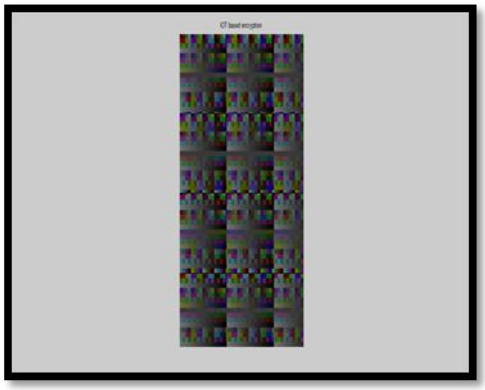

Fig. 8 Encrypted input image through IOT

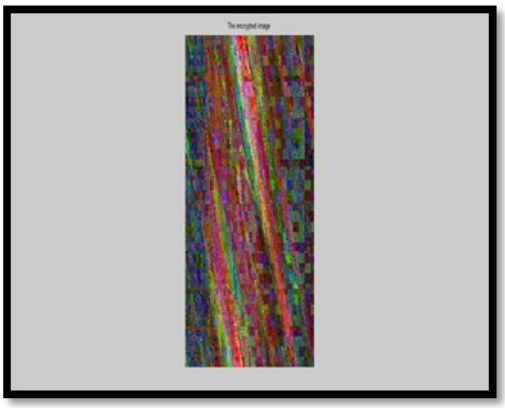

Fig. 9 Final encryption

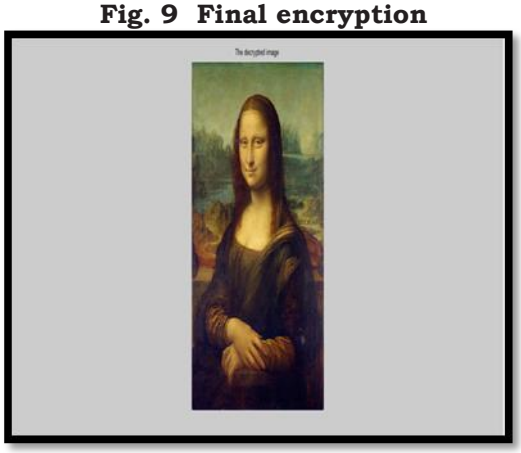

Fig. 10 Decryption of input image

6 RESULT DISCUSSION WITH DISCRIPTION

An encryption algorithm discussed in base paper is composed of several computational rounds that may occupy significant memory making it unsuitable to be utilized in IoT encryption. The proposed algorithm is evaluated in terms of its memory utilization.

The proposed algorithm utilizes the 22 bytes of memory on AT mega 328 platform While for DNA encryption the software environment is MATLAB2014a,

The hardware environment is the win7 system, the processor is i5, the RAM is 4GB, and the hard disk is PC with 500G.

With the above simulation environment, simulation and analysis are carried out for the secret key, the entropy of information, the anti-differential ability, and the ability against statistical attack Proposed work based on IOT has five rounds of calculation which makes proposed method better than DNA based image Encryption.

The execution time is found to be 0.188 milliseconds and 0.187 milliseconds for encryption and decryption respectively which is less than DNA based methodology which has more rounds consumes more time.

DNA encryption gets the entropy of information: 7.9979 which is closed to IoT based entropy around 7.9977 but memory cost and run time consume more than IoT.

Comparison with Old Algorithm

Parameter of Comparison	DNA algorithm	AES for IOT algorithm	Outcome
Correlation	0.0152(High)	0.0015 (low)	Excellent than DNA
Memory cost	RAM4G(Cost High)	ATmega328Low cost	Excellent than DNA
Ease of Operation	Complex	Easy	Fast and secure than old algorithm

7 CONCLUSION

We tested the algorithm for computational resource utilization and computational complexity. We observe the memory utilization and total computational time utilized by the algorithm for the key generation, encryption and decryption. The required hardware implementation of the algorithm is done on a Motorola based 64-bit micro-controller for higher speed.

We proposed three novel path selection methods, namely, SPS protocol, RPS protocol, and BPS protocol to investigate the impact of EH and hardware impairments on the outage performance of multi-hop multi-path cooperative WSNs. Moreover, we derive exactly and asymptotically the outage probabilities of three proposed protocols under the presence of one beacon, multiple eavesdropping attacks.

The simulation results verified that the employment of BPS together with multi-hop multi-path schemes can enhance significantly the secure performance of the considered EH and hardware impairment system. In particular, BPS is more robust to hardware impairment than RPS and SPS; thus, it can operate better with device that has a poor hardware quality

REFERENCES

1. KONG Liuyong, LI Lin "A new image encryption algorithm based on Chaos Proceedings of the 35th Chinese Control Conference July 27-29, 2016,
2. J. Romero-Mariona, R. Hallman, M. Kline, J. San Miguel, M. Major, and L. Kerr, "Security in the industrial internet of things," 2016.
3. G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song, and D. Wagner, "Smart locks: Lessons for securing commodity internet of things devices," in Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. ACM, 2016, pp. 461–472
4. D. Airehrour, J. Gutierrez, and S. K. Ray, "Secure routing for internet of things: A survey," Journal of Network and Computer Applications, vol. 66, pp. 198–213, 2016.
5. P. Zhao, T. Peffer, R. Narayanamurthy, G. Fierro, P. Raftery, S. Kaam, and J. Kim, "Getting into the zone: how the internet of things can improve energy efficiency and demand response in a commercial building," 2016.
6. S. Misra, M. Maheswaran, and S. Hashmi, "Security challenges and approaches in internet of things," 2016.
7. H. J. Ban, J. Choi, and N. Kang, "Fine-grained support of security services for resource constrained internet of things," International Journal of Distributed Sensor Networks, vol. 2016, 2016.
8. P. L. L. P. Pan Wang, Professor Sohail Chaudhry, S. Li, T. Tryfonas, and H. Li, "The internet of things: a security point of view," Internet Research, vol. 26, no. 2, pp. 337–359, 2016.
9. F. Xie and H. Chen, "An efficient and robust data integrity verification algorithm based on context sensitive," way, vol. 10, no. 4, 2016.
10. M. A. Simplicio Jr, M. V. Silva, R. C. Alves, and T. K. Shibata,"Lightweight and escrow-less authenticated key agreement for the internet of things," Computer Communications, 2016
11. R. Want and S. Dustdar, "Activating the internet of things [guest editors' introduction]," Computer, vol. 48, no. 9, pp. 16–20, 2015.
12. M. Ebrahim, S. Khan, and U. Khalid, "Security risk analysis in peer 2 peer system; an approach towards surmounting security

challenges," arXiv preprint arXiv: 1404.5123, 2014.

13. S. Wang, Z. Zhang, Z. Ye, X. Wang, X. Lin, and S. Chen, "Application of environmental internet of things on water quality management of urban scenic river," International Journal of Sustainable Development & World Ecology, vol. 20, no. 3, pp. 216–222, 2013.
14. Z. Pang, Q. Chen, J. Tian, L. Zheng, and E. Dubrova, "Ecosystem analysis in the design of open platform-based in-home healthcare terminals towards the internet-of-things," in Advanced Communication Technology (ICACT), 2013 15th International Conference on. IEEE, 2013, pp. 529–534.