


TDSJ–IoT: Trivial Data Transmission to Sustain Energy From Reactive Jamming Attack in IoT

Ambika N.

 <https://orcid.org/0000-0003-4452-5514>

Department of Computer Application, SSMRV College, Bangalore, India

INTRODUCTION

Internet-of-things (Stankovic, 2014) is a combination of sensor technology with Radio Frequency Identification Device (RFID) (Jia, 2012) (Fan, Gong, Du, Li, & Yang, 2015), Geological Information System (GIS) (Liu, 2014) (Lopez, Lopez, Prieto, & Quinde, 2017) and Global positioning system (GPS) (Kumar, 2017) (Mala, Thushara, & Subbiah, 2017) (Jisha, Jyothindranath, & Kumary, 2017). The devices communicate with each other using integrated technology. The integration has aided to improve the quality of one's life minimizing human efforts. The technology consisting of a variety of devices aims to think, hear which aid in their doings and share information with each other. Four components are used to do the same. Sensing, heterogeneous access, information processing, applications, and services come together to bring the technology into play. The devices using the underlying technology turn the doings to become smarter. The applications include transportation (Melis, 2016) (Masek, et al., 2016), agriculture (Mat, 2016) (Popović, 2017), industry automation (Shrouf, 2014), emergency response (Yang, 2013) (Rathore, 2016) and healthcare (Muhammad, 2017) (Mano, 2016). Security (Andrea, 2015) and privacy components can be added to make the technology better.

Security in these devices is one of the prior issues to be considered as these devices will not be under continuous supervision. Hence the devices are liable to different kinds of attacks. Jamming attack (Alaba, 2017) (Kasinathan, 2013) is one such attack where the packets dispatched to the destination is hindered to reach the same. This leads to loss of packets and rarely the packets may reach the destination improperly. Many kinds of jammers are available. This includes basic jammers – reactive jammers, constant jammers, deceptive jammers, and random jammers. The second category of jammers namely intelligent jammers is of two kinds - statistical jammers and protocol-aware jammers. Each jammer has different characteristics and is active on different layers of the network. The descriptions of them are narrated in section 2.

The proposed work minimizes reactive jamming attack (Grover, 2014) (Babar, 2013) in the network. The work adopts some precautions to be taken to identify the adversaries before in hand. The methodology used will be able to detect the intruder earlier in the stage. Three kinds of precautions are taken in the proposed work. First, the devices are to sense the channel before commencing communication with any other device. They will be in continuous vigilance monitoring their surroundings. Second, to find the appropriate route, the device broadcasts sample bits addressing the receiving device. The reactive adversary sensing the packets are liable to transmit its packets. Hence the packets of the legitimate source will not reach the desired destination or will take a lot of time to reach its destination. The receiver affixes the time and path from which the packet it has received. Using this information the

DOI: 10.4018/978-1-7998-3479-3.ch038

further communication path is set. As the device is continuously sensing the channel it will be able to figure out jammers to some extent. Third, every device dispatching the packets will be equipped with device-id. Using the device-id, a hash code is derived which uniquely identifies the device. The hash code is prefixed to the transmitted packets. The receivers analyze the prefixed code along with signal strength and continuous with the communication if found legitimate. Using these steps reliability to the communication is increased by 4%, the effectiveness is increased by 7.6% and energy is minimized by 6.3% compared with the previous work.

The work is divided into eight sections. The introduction to the work is provided in section 1. Different kinds of jamming attacks are detailed in section 2 and Literature survey is explained in section 3. Section 4 contains the detailing of the proposed work. The details of the simulation are done in NS2 is provided in section 5 and the analysis of the same is provided in section 6. Section 7 details the future work to be taken. The work is concluded in section 8.

JAMMING ATTACKS

Different kinds of jamming attacks are available. Two kinds of jammers are available. They are basic and intelligent jammers (Hamza, 2016) (Noubir, 97-108). The basic jammers are into dispatching the packets are different intervals of time continuously or discreetly. Basic jammers are of four kinds- namely constant jammers, random jammers, deceptive jammers, and reactive jammers. The intelligent jammers are designed to understand the underlying technology and implement jamming to hinder the transmission. Intelligent jammers are of two kinds namely statistical jammer and protocol-aware jammer. Their characteristics are detailed in Table 1.

Table 1. Characteristics of different kinds of Jammers

Type of jammers		Characteristics
Basic jammers	Constant jammers (Han, 2018)	<ul style="list-style-type: none"> · This kind of jammer is effective on physical layer. · The jammer transmits continuous random bits without following any MAC label.
	Deceptive jammers (Lee, 2014)	<ul style="list-style-type: none"> · This kind of jammer is effective in MAC layer · The adversary continuously inject regular packets without any interval between packet transmission
	Random jammers (Wei, 2014) (Sanguanpong, 2018)	<ul style="list-style-type: none"> · The jammers toggle between sleep and jamming state. · This kind of jammer is effective in MAC layer
	Reactive jammers (Fadele, 2018) (Sciancalepore, 2018)	<ul style="list-style-type: none"> · This kind of jammer is effective in MAC layer · They emit radio signal on detecting any activity in the channel · These jammers keep the channel busy
Intelligent jammers	Statistical jammer (Ren, 2013)	<ul style="list-style-type: none"> · This kind of jammers are effective in physical layer · Observes the packet inter-arrival distribution and regulates itself to the traffic disrupting communication of the network
	Protocol-aware jammer (Sufyan, 2013) (Toledo, 2008)	<ul style="list-style-type: none"> · These kinds of jammers are effective in MAC layer. · It Keeps itself updated with the operating rules and deprives the legitimate nodes using its database.

11 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/tdsj-iot/260211

Related Content

An Efficient Image Retrieval Based on Fusion of Fast Features and Query Image Classification

Vibhav Prakash Singh, Subodh Srivastava and Rajeev Srivastava (2017). *International Journal of Rough Sets and Data Analysis* (pp. 19-37).

www.irma-international.org/article/an-efficient-image-retrieval-based-on-fusion-of-fast-features-and-query-image-classification/169172

Integrated Methods for a User Adapted Usability Evaluation

Junko Shirogane, Yuichiro Yashita, Hajime Iwata and Yoshiaki Fukazawa (2013). *Information Systems Research and Exploring Social Artifacts: Approaches and Methodologies* (pp. 379-397).

www.irma-international.org/chapter/integrated-methods-user-adapted-usability/70725

The Use of Geo-Spatial Technology in Handheld Devices for Teaching Geography in a Formal School Context

Pamela Cowan and Ryan Butler (2015). *Encyclopedia of Information Science and Technology, Third Edition* (pp. 2636-2646).

www.irma-international.org/chapter/the-use-of-geo-spatial-technology-in-handheld-devices-for-teaching-geography-in-a-formal-school-context/112680

Temperature Measurement Method and Simulation of Power Cable Based on Edge Computing and RFID

Runmin Guan, Huan Chen, Jian Shang and Li Pan (2024). *International Journal of Information Technologies and Systems Approach* (pp. 1-20).

www.irma-international.org/article/temperature-measurement-method-and-simulation-of-power-cable-based-on-edge-computing-and-rfid/341789

Concept and Practices of Cyber Supply Chain in Manufacturing Context

Anisha Banu Dawood Gani and Yudi Fernando (2018). *Encyclopedia of Information Science and Technology, Fourth Edition* (pp. 5306-5316).

www.irma-international.org/chapter/concept-and-practices-of-cyber-supply-chain-in-manufacturing-context/184234