 doi:10.20944/preprints202001.0303.v1

Securing Internet of Things Against Physical Layer Attacks Using Hybrid Security Algorithm (HSA)

Meysam Zarei [1] .

Abstract Through the Internet of Things (IoT) the internet scope is established by the aid of physical objects integration to classify themselves to mutual things. A physical object can be created by this inventive perception to signify itself in the digital world. Regarding the physical objects that are related to the internet, it is worth to mention that considering numerous theories and upcoming predictions, they mostly require protected structures, moreover, they are at risk of several attacks. IoTs are endangered by particular routing disobedience called physical layer attack owing to their distributed features. The physical layer attack as a security warning makes possible for the invader to abuse the resources and bandwidth of the network through overloading the network via unimportant packets. This protocol is called LSFA-IoT consisting of two key sections of the physical layer detection system and misbehavior detection system. The first section is utilized in stabilizing the status of the network. The second section is in charge of discovering the misbehavior sources within the IoT network through $APT-RREQ$, the Average Packet Transmission RREQ. By detecting a malicious node, the status of the node is checked by LSFA-IoT prior to sending a data packet and in case detecting the node as malicious, no packet is sent to that node and that node is added to the detention list. Here, the technique is assessed through wide simulations performed within the NS-3 environment. Based on the results of the simulation, it is indicated that the IoT network behaviour metrics are enhanced based on the detection rate, false-negative rate, false-positive rate, and packet delivery rate.

Keywords Internet of Things (IoT) . Physical layer attack . Routing security . Average Packet Transmission

✉ Meysam Zarei
Sm.zarei@khuisf.ac.ir

[1] Department of Computer, Isfahan (Khorasgan) Branch, Islamic Azad University, Isfahan 81595-158, Iran

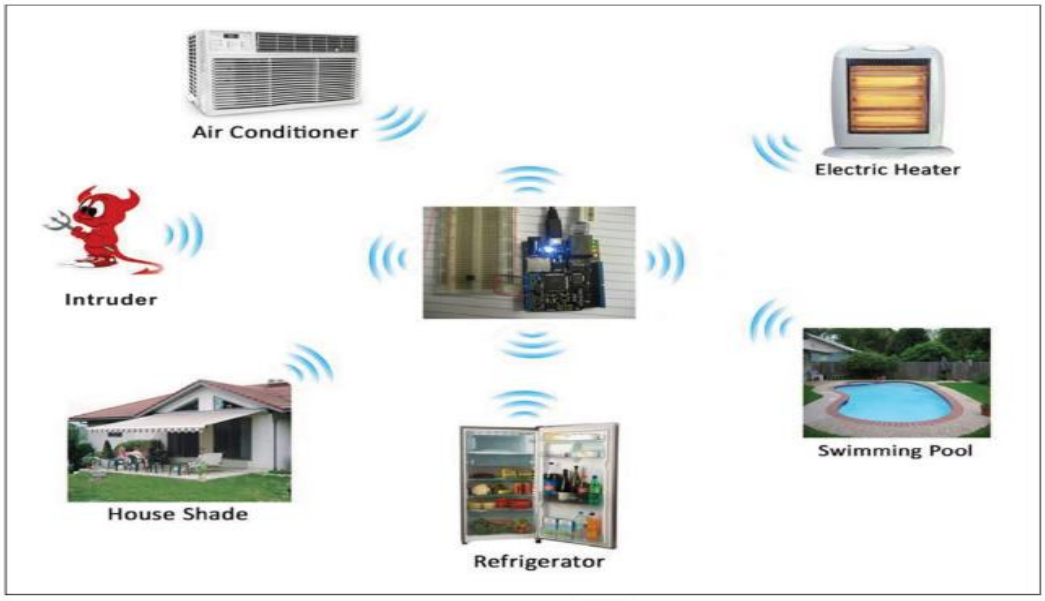
Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 January 2020 doi:10.20944/preprints202001.0303.v1

1 Introduction

The succeeding generation of internet services present everywhere and influencing all aspects of our diary life will be developed by numerous reasons including improvements in social network technologies, mobile and extending computing, and exponential evolution in Internet facilities. It can be expected that by 2031the number of IoT devices will surpass over 51 billion. However, despite the advantages of IoT through different applications, they are potentially vulnerable against risks as a result of circumstances, in which the actions are monitored by no pilot. It intensifies the necessity of designing reliable and secure IoT as well as overcoming the challenges to prevent mutilation and destruction to the other systems and human lives [1]. Some attacks like flooding attack (FA) enter the system illegally. By affecting attack in an IoT, it is difficult to remove the threat and make the system online again. It is worth to state that the usual approaches to secure information including intrusion detection or encryption, are not enough for coping with such risks. To elaborate, the stated outlines do not take into account the sensor and actuator measurements compatibility factor with the physical procedure and IoT's control mechanism that are considered in the protecting outline. Besides, problem of previous IoT systems was the mere attempt on eliminating a single attack type and were only resistant to it. If the system was subject to combined attack, it would be practically inoperative, and the intrusion operation would fail the system quickly.

In LSFA-IoT, we present a new security system that avoids producing unnecessary *RREQ* packets by malicious nodes. Our system can identify the attacks sending a large number of fake *RREQ* packets with invalid IPs to the destination. To detect these malicious nodes, we propose to implement a security module in each certified node in the network. We define two main parts in this mechanism: misbehavior detection system and flooding detection system. Figure 1 shows a vulnerable IoT connected scenario.

Fig. 1 A vulnerable IoT connected environment [2].



The paper presented here is organized as the following. Section 2 converses some relevant terms regarding application scenario, security attacks, detection schemes. In Sect. 3 brings the proposed LSFA-IoT strategy. In Section 4, the simulation results are discussed to demonstrate the efficiency

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 January 2020 doi:10.20944/preprints202001.0303.v1

of the proposed LSFA-IoT. Finally, conclusions and future works of this research are discussed in Section 5.

2 Relevant terms

This section provides an overview to the fundamental perceptions of this research work: application scenarios, security threats targeting IoT, and detection schemes to provide protection for the IoT.

2.1 Application Scenarios

There are a variety of areas composing of industry, municipal substructure, smart surroundings, and healthcare field for the application scenarios of the IoT (c.f. Fig. 2). These scenarios suffer the attacks that are various, cross-cutting across lots of procedures layers in IoT structural design, and containing incorporation of a diversity of attack techniques which will lead to increase the analyzing intricacy of the IoT security. In addition, the incentive of the attacker is probably different in various application scenarios, for instance, the target might be gain entrance to critical user data in a wearable application, despite the fact that healthcare-related attacks want to deteriorate the life safety of patients.

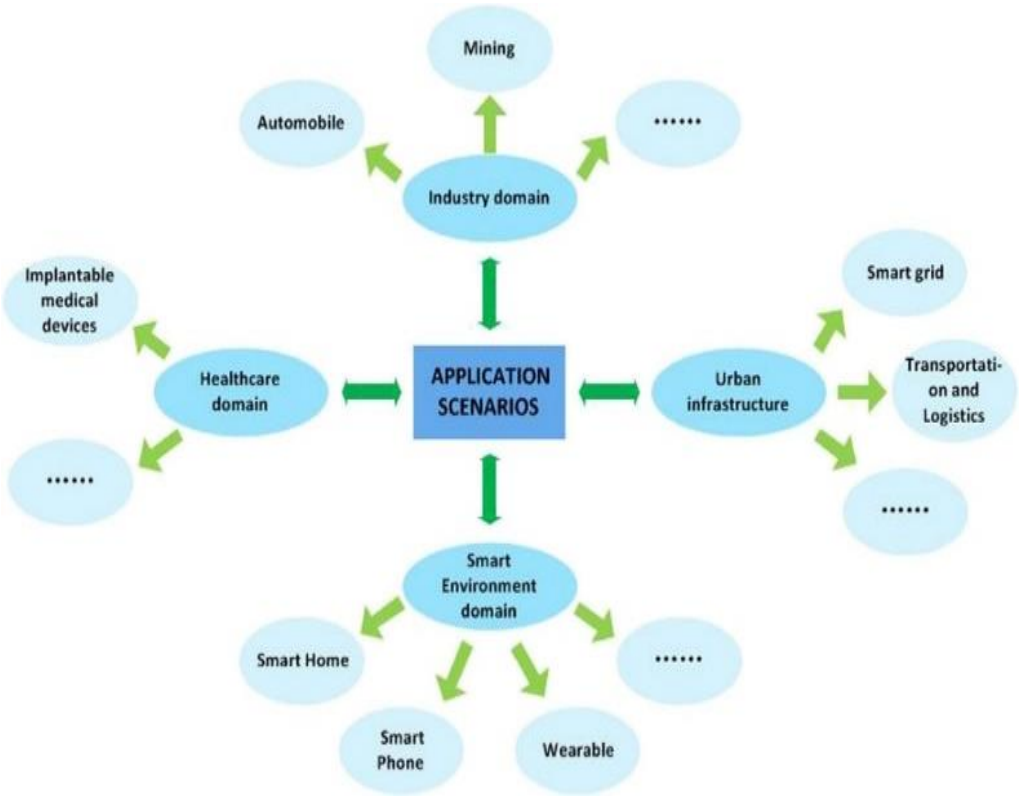


Fig. 2 Description of application scenarios in the IoT [2].

2.2 Security Attacks

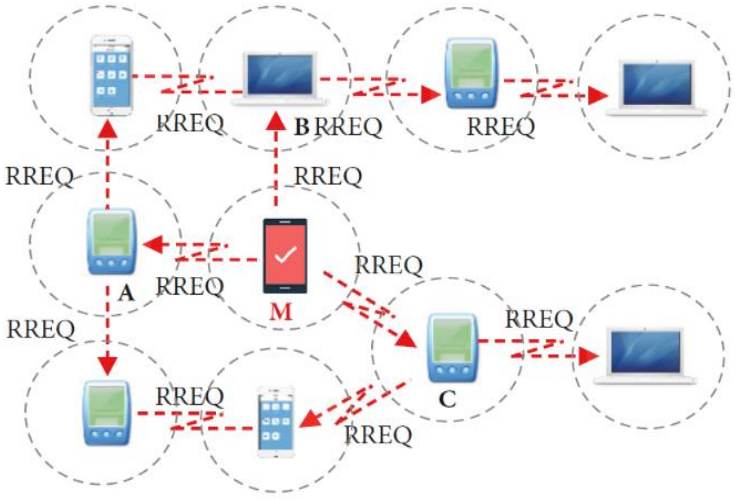
IoT Systems are vulnerable to function degradation and security risks. They might be passive or active threats as they have the reliance on wireless channels for communication. A security threat targeting IoT is provided in Figures 3. In this paper, the following vulnerability is of interest:

- *Flooding Attack* plays a key role in the security of IoT so that it is facile to begin; however, challenging to stop. A mischievous node can launch an attack with simplicity using sending an immoderately high number of route request (*RREQ*) packs or inoperable data ones to unreal

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 January 2020 doi:10.20944/preprints202001.0303.v1

destinations. Therefore, the network is rendered impractical so that all its resources are undermined to serve this hurricane of *RREQ* packs; as a result, it cannot carry out its standard routing responsibility [2].

Fig. 3 The flooding attacks in the IoT [2].



2.3 Detection schemes

Various security measurements have been developed and used in different works for addressing Denial of Sleep attacks, and protecting IoTs against gray hole attacks. It is not a recent issue, and there are extensive studies on it. Different approaches have been suggested by different studies in order to address these attacks.

To protect IoT sensors versus a huge amount of cyber-attacks, a methodology has been developed by Pacheco et al. [3]. At first, they presented the IoT security structure to SIs that involves 4 layers including devices (end nodes), network, services, and application. At that point, their methodology was exhibited in order to develop a general threat model for distinguishing the weaknesses in each layer and the potential countermeasures which can be spread out to diminish their taking advantage. It is worthy to note that authors indicated how it is possible an anomaly behavior analysis invasion detection system (ABA-IDS) established upon the discrete wavelet transform (DWT) develops to discover abnormalities that could be activated by means of attacks in contrast to the sensors in the first layer of our IoT structure.

A spectrum of challenges, attitudes, and practice in IoT security has been taken into account in [4]. IoT security is exclusive in several ways. Moreover, it lets us know about numerous experiments which are dissimilar from those in security guarantee of other computing devices like desktops, laptops, servers, or even mobile devices. They specially develop two classifications of security attacks with respect to the IoT system. The first one presents attacks on the four-layer structural design of IoT including perception, network, middleware, and application layer. On the foundation of that, they analytically investigated the security dangers and privacy concerns on every single layer of IoT. Because of occurring the attacks in each layer of IoT, the authors had to provide a security barrier for the whole IoT structure, not only for a particular technology. The second one of the IoT security and susceptibilities is dependent upon various application scenarios. The second classification creates a systematic basis to protect different IoT applications.

As a new public significant cryptography, Lattice-Based cryptography has been developed in [5] to substitute the public one. In order to execute lattice-based cryptography, the Ring-LWE scheme has been recommended. There should be an optimization for applying the scheme to the IoT devices via 8-bit, 32-bit, or 64-bit microcontrollers. It should be noted that the 8-bit environment is very significant for small IoT devices. Nevertheless, side-channel attacks can be damaged the Ring-LWE

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 January 2020 doi:10.20944/preprints202001.0303.v1

performance. In this research, using 8-bit microcontrollers, we analyze the attack scenarios and offer a countermeasure by bit examination for the IoT applications.

To validate and interconnect the main generation between the IoT devices, a lightweight physical-layer established security plan is recommended in [6]. They have scientifically examined and evaluated the developed method by considering the practicability of real executions. Additionally, they have comprehensively suggested a physical-layer main generation and identification scheme established upon frequency hopping communications as the RSSs of distinctive frequencies create its parameter sets.

The history, background, and statistics of IoT, also, security-based analysis of IoT architecture have been thoroughly discussed in [7]. Besides, they have provided two types of classifications including security challenges in the IoT environment and different protection mechanisms. They have also concluded that investigation on numerous research challenges, which exist in the literature yet, can provide a superior realization about the problem, present elucidation space, and upcoming research guidelines to protect the IoT versus the different attacks.

On the basis of elliptic curve cryptography (ECC), Alamr et al. [8] have recommended a new radio-frequency identification verification procedure in order to get rid of lots of weaknesses. As well, they have utilized elliptic curve Diffie–Hellman (ECDH) vital agreement procedure to generate a provisional shared key which is served to encrypt the future conveyed messages. Their procedure attains a set of security properties such as reciprocal confirmation, unrecognizability, secrecy, forward security, location privacy, and the withstanding against man-in-the-middle, replay and impersonation attacks.

The aforementioned IoT problems in the network security have been introduced and the requirement of invasion detection indicated in [9]. A number of categories of invasion uncovering technologies have been talked about and their application on IoT architecture has been studied. They have compared the application of various technologies and made a viewpoint of the following phase of research. The study of network invasion technology can be a crucial topic through data mining and machine learning approaches. More than one class feature or detection model is required to increase the exposure rate of network invasion uncovering.

The IoT security problem has been addressed in [10]. They want to obstruct the attacks at the network level rather than device one using SDN. Their goal was to defend the IoT devices from malevolent attacks and diminished the created damage. The attack is almost certainly begun by the IoT device itself or the device is the target. A framework and soft things for the IoT security established upon the SDN methods, which assists in quick recognition of unusual behavior and heightened flexibility, have been presented in [10]. They have executed the concept proof on Mininet emulator in order to distinguish irregular traffic of IoT with a Support Vector Machine (SVM), machine learning algorithm, and succeeding alleviation of the attacks. Moreover, they have taken into account lots of attacks such as TCP and ICMP flooding, DDoS, and scenarios alongside the IoT device as both target and source of attacks. We compare the linear and nonlinear SVM performance in the aforementioned scenarios for the detection of these attacks.

Rostampour et al. [11] have developed an original grouping proof procedure which can be scaled. Since the scalability is a challenge in grouping proof procedure, the reader individualistically publicizes its messages and tags in order to resolve the scalability problem in the recommended procedure. To evaluate the performance of the novel technique, they have served a 64-bit lightweight Pseudo-Random Number Generator (64-PRNG) function which satisfies the requirements of low-power and low-cost systems.

To confirm the security technology, a test bed has been fabricated to discover the potential cyber-attacks in the next-generation intelligent power control system environment which is defined like IEC

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 January 2020 doi:10.20944/preprints202001.0303.v1

and NIST in standard documents and directed the investigates to approve the appropriateness of the test bed [12]. The suggested test bed can steadily integrate the new security technologies into the industrial important substructure. Besides, it is also predictable that system security and steadiness will be improved.

This work suggested constructing a trust-oriented framework for RPL to counter blackhole attacks. It can be run at two levels of an intra-DODAG and an inter-DODAG. Incremented dropping the packets, depleting the resources, and high packet overhead are the impacts of blackhole attacks in an IoT network. It eventually leads to destabilizing the network owing to incremented packet delay, rank modifying and disturbance in the topology. Regarding the rank modifying, the ranks are computed again, therefore, activating a local repair later initiating a repair thoroughly by the root. Such regular repairs might end up influencing the network efficiency [13].

The nodes mobility problem has been scrutinized so that the recommended solution has an appropriate performance in portable environments [14]. Their security mechanism is founded on the reliance concept. Reliance is a level of security that every single thing has from the other things for achievement in the demanded job without leading to security complications. To reliance things in the IoT having a multi-dimensional visualization of the reliance, they have provided a widespread hierarchical model. The three most key dimensions that should be taken into account are as follows: quality of p2p communication and service and background information. These dimensions and lively and versatile techniques, which are utilized in the calculation of the reliance and provided a mechanism in order to serve the computed reliance, make available security necessities to handle the attacks in the IoT movable environment despite the fact that network performance increases. It is worthy to mention that these dimensions are not restricted and the model has the aptitude to take into account the other ones on the foundation of the calculation purpose of the reliance. In the developed technique, they have incorporated the reliance model into RPL and provided an innovative OF. The recommended new RPL procedure was experimentally assessed under attacks of BLACKHOLE, SYBIL, and RANK in connection with subsequent performance metrics as packet loss rate, end-to-end delay, and average parent variations.

This research work is intended to implement a new methodology, i.e. profound learning, related to the cybersecurity to facilitate the attacks revealing in the public internet of things. The profound model performance has been compared to the traditional machine learning method, also, the distributed attack detection (DAD) has been assessed versus the concentrate uncovering system [15].

In the presence of three individual packets dropping attacks, a sensitivity analysis of TRS-PD preformed through a change of different parameters values in various network scenarios have been accomplished in [16]. Moreover, this work was a summary of the attack-pattern detection mechanism, reliance model, and routing mechanism adopted by TRS-PD to withstand the opponents which follow the specific attack patterns accompanied by the other ones.

A lightweight reciprocal validation established on the scheme has been suggested for the real-world physical objects of an IoT environment. It is a payload-founded encryption scheme which serves an uncomplicated four-way handshake mechanism in order to confirm the individualities of the contributing objects. It should be expressed that the real-world objects interconnect to each other by means of the client-server interaction model. Their developed scheme utilizes the lightweight characteristics of the Constrained Application Protocol (CoAP) to make a condition that the customers can perceive resources existed within the server in an energy-effective routine. They have utilized the Advanced Encryption Standard (AES) with a strategic length of 128 bits to found a protected assembly for resource observation. They have assessed their scheme in a real-world scenario with NetDuino Plus 2 boards [17].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 January 2020 doi:10.20944/preprints202001.0303.v1

The problem of conspiracy attacks in the IoT environments and how the movement of the IoT devices increases the hardship of discovering such categories of attacks have been studied in [18]. It proves that the applied methods in detecting the conspiracy attacks in WSNs are not applicable in IoT environments. As a final point, the current research introduces a model established upon Fog Computing substructure to preserve IoT devices path and identify the conspiracy attackers. This model employs a fog computing layer for real-time monitoring and uncovering of the conspiracy attacks in the IoT environments.

Zakaria et al. [19] have impressed via the SDN abilities as they have presented a complete review of obtainable SDN-based DDoS attack uncovering and alleviation solutions. According to the DDoS attack discovery, they have categorized solutions techniques and determined the necessities of an operational solution. Furthermore, on the basis of their outcomes, they have recommended an original framework for uncovering and alleviation of DDoS attacks in a large-scale network which composes of a smart city built on the SDN substructure. Their recommended framework is able to satisfy the application-specific DDoS attack discovery and alleviation needs. The most important involvement is double. First, they have provided a detailed investigation and argument of SDN-based DDoS attack discovery and alleviation mechanisms, also, they have categorized them regarding the discovery methods. Second, by leveraging the SDN features for the network security, they have recommended and developed an SDN-established proactive DDoS Defense Framework (ProDefense).

A basis location security procedure based on dynamic routing addresses the source location confidentiality problem. The authors have introduced a self-motivated routing scheme which aims at maximizing tracks for data broadcast. At first, the suggested scheme arbitrarily selects a preliminary node from the network boundary. All of the packages will make a journey through an avaricious and successive directed route before attainment to the sink [20].

MLDMF has been presented for IIoT in [21] which comprises the cloud, fog, and edge computing level. Software-defined networking (SDN) has been utilized to manipulate the network. These two frameworks are combined to advance access security and effectual controlling of IIoT.

A method called REATO has been presented to identify and neutralize a DoS attack in contrast to the IoT middleware known as NPS. The premeditated solution tailored to the NPS architecture has been authenticated using a real test-bed and composed by a NPS sample mounted on a Raspberry Pi that receives open data feeds in real time via an adaptable set of sources. The work started from the obligation to find out a solution is capable of to guard an IoT system towards DoS attacks by considering all the potential circumstances that can take place (i.e., attacks to the data sources and attacks to the IoT platform) [22].

A deep-learning established machine learning method has been presented in [22] for the IoT to detect the routing attacks. The Cooja IoT emulator has been employed to generate high-fidelity attack data within IoT networks having 10 to 1000 nodes. They have recommended a highly scalable, profound-learning based attack detection approach to uncover the IoT routing attacks which are decreased rank, hello-flood, and version number modification attacks through extraordinary accurateness and meticulousness. Applying the deep learning for cyber-security in the IoT necessitates the accessibility of considerable IoT attack data.

Table 1 recapitulates the performed efforts in order to design IDS for the IoT (”-” stands for an indefinite characteristic).

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 January 2020 doi:10.20944/preprints202001.0303.v1

Table 1 Summary of the IDS for IoT literature.

References	Placement schema	Detection schema	Attack type	Validation schema
[3]	Centralized	Anomaly-based	DoS	_*Simulation*
[4]	Hybrid	Hybrid	Routing attack	_*Simulation*
[5]	Distributed	Signature-based	Side-channel attack	_*None*
[6]	Hybrid	Hybrid	Physical-layer attack	_*Simulation*
[7]	Hybrid	Hybrid	Multiple conventional attacks	_*Simulation*
[8]	Distributed	Signature-based	MIMA, replay and impersonation attack	_*Simulation*
[9]	–	Signature-based	Multiple conventional attacks	_*Empirical*
[10]	Centralized	Anomaly-based	DDoS	_*Empirical*
[11]	–	Signature-based	RFID attacks	_*None*
[12]	–	Anomaly-based	Cyber-attacks	_*Simulation*
[13]	Centralized	Anomaly-based	DDoS	_*Simulation*
[14]		Signature-based	Routing attacks	_*None*
[15]	Distributed	Signature-based	Distributed attack	_*Simulation*
[16]	Centralized	Anomaly-based	Packet dropping attacks	_*Empirical*
[17]	–	Anomaly-based	Replay Attack	_*Simulation*
[18]	Distributed	Signature-based	Collusion attacks	_*None*
[19]	–	Anomaly-based	DDoS	_*Simulation*
[20]	Distributed	Signature-based	Cyber-attacks	_*Empirical*
[21]	–	Anomaly-based	DDoS	_*Simulation*
[23]	Centralized	Anomaly-based	DoS	_*Simulation*
[22]	Hybrid	Signature-based	Routing attacks	_*Simulation*

In Table 2, a comparison of detected attacks and categories in the literature is highlighted.

Table 2 Security threats detection schemes for IoT.

Proposed system	Detected attacks	Category
Pacheco et al. (2017)	variety of cyberattacks	DoS
Chen et al. (2018)	Network layer attacks	Routing attack
Moon et al. (2018)	Side-channel and power analysis attack	Side-channel attack
Jiang et al. (2018)	physical-layer security	Physical-layer attack
Adat et al. (2017)	An energy consumption model for detecting of the DoS	Multiple conventional attacks
Alamr et al. (2016)	MIMA, replay and impersonation	MIMA, replay and impersonation
Deng et al. (2018)	hijack attack	Multiple conventional attacks
Bhunia and Gurusamy (2017)	malicious attacks	DDoS
Rostampour et al. (2017)	RFID attacks	RFID attacks
Lee et al. (2017)	Stuxnet attack	Cyber-attacks
Qin et al. (2019)	DDoS	DDoS
Hashemi et al. (2018)	Cyber-attack	Routing attacks
Diro and Chilamkurti (2017)	Topology attacks on RPL	Distributed attack
Jhaveri et al. (2018)	Sinkhole and neighbor attacks	Packet dropping attacks
Jan et al. (2017)	Cyber-attack	Replay Attack
Yaseen et al. (2017)	Packet forwarding misbehavior	Collusion attacks
Bawany et al. (2017)	DDoS	DDoS
Han et al. (2017)	eavesdropping, hopby and direction-oriented attack	Cyber-attacks
Yan et al. (2018)	multi-level DDoS	DDoS
Sicari et al. (2018)	Denial of Service (DoS) attack	DoS
Yavuz et al. (2018)	Cyber security	Routing attacks

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 January 2020 doi:10.20944/preprints202001.0303.v1

3 The proposed LSFA-IoT schema

In the following section, we design a flooding-security threats-immune schema by employing the *APT – RREQ* algorithm. The LSFA-IoT consists of six steps, such as the assumptions of the proposed LSFA-IoT method is discussed in Sect, 3.1. Overview of the LSFA-IoT schema is discussed in Sect, 3.2. Misbehavior notification step is discussed in Sect. 3.3, the mechanism to detect physical layer attack in LSFA-IoT is discussed in Sect. 3.4, Adding the malicious thing to detention list is discussed in Sect. 3.5, and revision of malicious thing is discussed in Sect. 3.6.

4.1 The assumptions of the proposed LSFA-IoT method

The parameters that we have considered for our proposed method are as follows.

- There isn't any central controller in the IoT network.
- All the things in the IoT network act as a final system and router for sending packets.
- All the things in the IoT network are mobile.
- The connections between the things are done by the AODV [24] protocol.
- Things should follow the standard protocol to join or left.

4.2 Overview of the LSFA-IoT schema

The proposed LSFA-IoT method is designed for the IoT based on the AODV protocol. LSFA-IoT is based on the analysis and prevention of the flooding attack in the network layer in IoT. The LSFA-IoT is based on the neighbor suppression technique which detects the malicious thing during the route building step. In the case of finding a malicious thing, the proposed method keeps that solitary for a while and checks its behavior to avoid flooding attack in the network layer. Before sending a packet, each node checks the detention list field in LSFA-IoT. If the thing is in the detention list, the packet will not be sent to, otherwise, the node is considered normal and the packet will be sent to.

In LSFA-IoT, we present a new security system that avoids producing unnecessary *RREQ* packets by malicious nodes. Our system can identify the attacks sending a large number of fake *RREQ* packets with invalid IPs to the destination. To detect these malicious nodes, we propose to implement a security module in each certified node in the network. We define two main parts in this mechanism: misbehavior detection system and flooding detection system.

The first part is used to stabilize the status of the network. If the number of route requests exceeds the threshold, we will make these nodes aware of misbehavior and abnormal behavior in the network. This notification indicates one or more *RREQ* flooding attack in the network and causes the second part to run.

The duty of the second part is to discover the misbehavior sources in the network that can be a single attack or common torrent attacks. Such attacks can be detected based on the immediate routings of the different packets sent/received by each existing node. The AODV protocol uses a voluntary *Hello* message for the stability of the connections between the neighbor nodes. We use the *Hello* packet to send information like starting route discovery by network nodes. All the nodes must observe all the mechanism defined to avoid creating fake route requests in the network.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 January 2020 doi:10.20944/preprints202001.0303.v1

4.3 Misbehavior notification step

The misbehavior notification step is used to optimally detect the misbehavior of the nodes and contribute to creating active security solutions. The detection system is inactive as long as the network is in secure status and no flooding attack is reported. To address the network status, every node exchanges the *Hello* message with its neighbors through a defined process.

We add a new field to *Hello* message that provides some information about produced or received *RREQ* packets. In fact, each node raises the number of its received messages by one (received++) after receiving a *RREQ* message and raises the number of its sent messages by one (sent++) after sending a *RREQ* message. Using this field guarantees the periodic tracing of the nodes behavior to check whether they are part of a flooding attack or not. Every node must contain the information of the *Hello* message about the exchanged *RREQ* packets. The *Hello* message is used not only to stabilize the connections between the neighbor nodes but also to check whether the network is secure regarding flooding attacks or not. Before sending the *Hello* message, nodes produce and receive some information about *RREQ* messages during sending the *Hello* message.

When a *Hello* message is received from a neighbor node, the receiving node marks its neighbor node as an active node and decodes the existing information in the *Hello* message. If the neighbor node is a new node, the receiving node creates a new input to record the information of this node in its table and writes the information of the node on but if it is a repetitive node, the receiving node updates the inputs related to. The node receiving the *Hello* message records every input in the table related to the neighbor which is selected as an active node and saves the information related to the exchanged *RREQ* packets. We assume that the unusual increased number of sent *RREQ* packets implies a flooding attack. We determine these unusual changes using the average transmission weight obtained from previous observations. If this weighted average exceeds the threshold, a detection process should be triggered by the attack detection system to detect the source of flooding attacks.

4.4 The mechanism to detect physical layer attack in LSFA-IoT

In the second step of our proposed LSFA-IoT method, the malicious nodes producing fake *RREQ* packets in the network are detected. As mentioned earlier, to run this step, we should first detect the misbehaviors in the network. The separation of these two steps has made the operations required for malicious node detection optimized. After running the detection process, every node should search the list of its neighbors to find the neighbor that has produced a large number of *RREQ* packets. To detect the source of flooding attacks, each node calculates the number of produced *RREQ* s. To do this, we use a weighted average formula in the LSFA-IoT. Average Packet Transmission *RREQ* ($APT - RREQ$) is used to calculate the average transmission of *RREQ* packets. The average transmission is used by series data in a certain period to smooth the specified short-term and long-term fluctuations. We analyze our observations about *RREQ* packets in a period using these calculations. $APT - RREQ$ may be calculated recursively for X series. Eq. (1) demonstrates the calculation.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 January 2020 doi:10.20944/preprints202001.0303.v1

$$\begin{cases} S_1 = X_1 & for\ t = 1 \\ S_t = \alpha * X_t + (1-\alpha) * S_{t-1} & for\ t > 1 \end{cases} \quad (1)$$

Where: $\begin{cases} \alpha\ is\ a\ smoothing\ \ factor\ \ (as\ a\ constant\ value\ between\ 0\ and\ 1). \\ X_t\ \ is\ the\ value\ of\ RREQ\ in\ period\ t. \\ S_t\ \ is\ a\ value\ of\ APT-RREQ\ in\ each\ period\ t. \end{cases}$

According to the proposed method, we use different values of α to detect flooding attacks. The $APT-RREQ$ can be applied with the low values of α to check network when it is under a flooding attack. However, the high values of α can help to analyze the general observations of the network in a certain period and detect attack source. The number of sent *RREQ* is determined for each node after information acquisition using the *Hello* message. Each node calculates $APT-RREQ$ value for its neighbor nodes by receiving a *Hello* message from them and getting the information of the neighbor node. We consider a threshold for $APT-RREQ$ each time. If the value of $APT-RREQ$ or a node exceeds the threshold, it indicates that the number of the *RREQ* messages transmitted by this node is far more than the expected threshold. Therefore, this node is detected as malicious.

4.5 Adding the malicious thing to detention list

When a thing detects a malicious neighbor thing, it adds that thing to its detention list and rejects all the requests received from that thing for a period of θ. Also, it sends a *RREQ* to its neighbors to eliminate their connections with the malicious thing and isolate that from the network for a period of θ.

4.6 Revision of malicious thing

Each thing maintains the detention list field for $\theta = 4 * RTT$ where RTT is the average round trip time of *RREQ*. When this time is over, the invalid node is considered valid and is used during the normal operations of the network. when a node is considered as a valid or normal node, all neighbor nodes update the LSFA-IoT inputs related to this node. If a duplicate node shows malicious behavior again, it will be placed in detention list again and all neighbor nodes make the changes in LSFA-IoT based on. As observed, we introduced our proposed LSFA-IoT method which is a useful method to detect flooding attacks in IoT. The flowchart of proposed LSFA-IoT is given in Fig. 4.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 January 2020 doi:10.20944/preprints202001.0303.v1

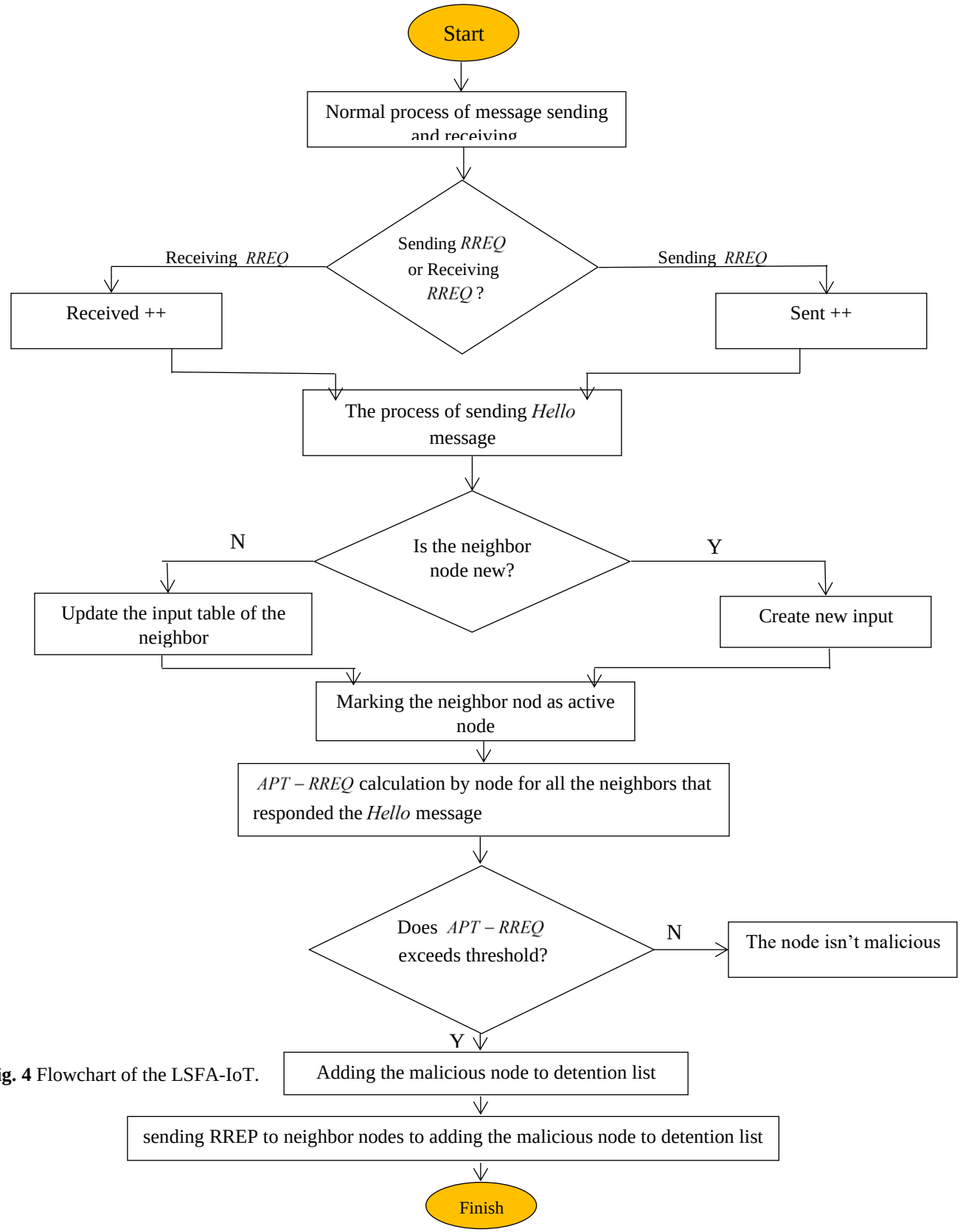


Fig. 4 Flowchart of the LSFA-IoT.

4 Evaluating the Performance

The LSFA-IoT performance is assessed in the following section to avoid the flooding attacks.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 January 2020 doi:10.20944/preprints202001.0303.v1

5.1 Performance metrics

Here, the performance and effectiveness of our suggested LSFA-IoT method are systematically assessed with complete simulations. A comparison is performed between the results and with REATO and IRAD methods proposed in [23] and [22], respectively. The PDR, false negative, false positive, and detection ratio are assessed. The meaning of notations used in the equations are given in Table 3.

Table 3 The parameters specified for *PDR*.

Notations	Means
X_i	Number of packets received by node i
Y_i	Number of packets sent by node i
n	Experiments

Table 4 Abbreviated notations

Parameters	Description
FPR	False positive rate
FNR	False negative rate
TPR	True positive rate
TNR	True negative rate
DR	Detection rate
PDR	Packet delivery rate
X_i	Denote the number of packets received by thing I
Y_i	Denote the number of packets sent by thing I

5.1.1 FPR

The FPR is calculated by the total number of nodes wrongly detected as the malicious nodes divided by the total number of normal nodes [25]. Therefore, the is defined as illustrated in Eq. (2).

$$FPR = \left(\frac{FPR}{FPR+TNR}\right)*100 \quad \text{Where:} \quad TNR = \left(\frac{TNR}{TNR+FPR}\right)*100 \tag{2}$$

5.1.2 FNR

The rate of the malicious node to total normal nodes that were mistakenly marked as a normal node [25]. Eq. (3) demonstrates the calculation.

$$FNR = \left(\frac{TPR+TNR}{All}\right)*100 \quad \text{Where:} \quad TPR = \left(\frac{TPR}{TPR+FNR}\right)*100 \tag{3}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 January 2020 doi:10.20944/preprints202001.0303.v1

5.1.3 *Detection rate*

It is determined as the ratio of the number of lethal attack nodes marked to the total number of existing lethal attack nodes in the IoT. DR is calculated by Eq. (4). Table 5 lists the parameters used for DR [26].

Table 5 The parameters specified for *DR*

Parameters	Description
TPR	The *TP* is obtained from the whole number of marked lethal attack nodes divided by the whole number of the lethal attack nodes.
FPR	The *FP* is obtained by the total number of nodes improperly recognized as the lethal attack nodes divided by the whole number of normal nodes.
TNR	The rate of the lethal attack nodes being properly marked as a lethal attack node.
FNR	The rate of the lethal attack node to whole normal nodes being wrongly marked as a normal node.

$$DR = \left(\frac{TPR}{TPR + FNR} \right) * 100 \quad \text{where} \quad All = TPR + TNR + FPR + FNR \tag{4}$$

5.1.4 *Packet delivery rate*

As defined, *PDR* results from dividing the total received packets of data at the destination UAV, to the total transmitted packets of data by the source UAV, denoted in percentage [26]. Eq. (5) demonstrates the average obtained PDR for n experiments.

$$PDR = \left(\frac{1}{n} \right) * \left(\frac{\sum_{i=1}^{n} X_i}{\sum_{i=1}^{n} Y_i} \right) * 100\% \tag{5}$$

5.2 Simulation setup and comparing algorithms

Because of the difficulty in debugging and implementing UAVNs in real networks, it is necessary to view simulations as a basic design tool. The primary benefit of simulation is that analysis is simplified and protocol is verified, mostly, it is evident in systems in large scales [27,28]. The performance of the suggested method is assessed in this part by the use of NS-3 as the simulation means, and the discussion on the obtained results is presented. It should be noted that it is assumed that all LSFA-IOT, REATO and IRAD settings and parameters are equal.

5.3 Simulation results and Analysis

In this section, we analyze the security performance of LSFA-IoT under the four attack scenarios (described in Table 6). This attack is categorized into lethal attacks. There are 500 UAV nodes uniformly deployed in the network area initially. Some important parameters are listed in Table 5.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 January 2020 doi:10.20944/preprints202001.0303.v1

Table 6 Setting of simulation parameters.

Parameters	Value
Coverage area (m x m)	First scenario: 2000 x 2000 Second scenario: 4000 x 4000
Simulation tool	NS-3
MAC	IEEE 802.11
Transport	UDP/IPv6
Range of communication	300 m
Bandwidth	3 Mbps
Traffic type, rate	CBR, 10 packets/sec
Model of mobility	Random way point
RX and TX ratio	90%
Number of nodes, and Packet size	500, 256 Kbps
Number of connections, and Pause time	50, 100 sec
Maximum mobility (varying)	5 m/sec - 25 m/sec
Percentage of malicious nodes	0% - 30%
Simulation time (varying)	500-2000

Table 7-10 compares the performance of LSFA-IoT with that of REATO and IRAD in terms of FPR, FNR, DR and PDR.

Table 7 *DR* (in %) of various frameworks with varying degree of malicious nodes.

Misbehaving thing ratio	Detection rate (%)		
	IRAD	*REATO*	*LSFA – IoT*
0	91.63	90.2	97.5
0.05	89.49	88.57	96.2
0.10	80.46	81.8	94.38
0.15	73.35	76.37	92.27
0.20	63.19	70.43	90.28
0.25	50.34	66.16	87.7
0.30	46.14	60.67	84.4

Table 8 FNR (in %) of various frameworks with varying degree of malicious nodes.

Misbehaving thing ratio	FNR (%)		
	IRAD	*REATO*	*LSFA – IoT*
0	7.93	9.005	2.34
0.05	8.43	10.08	2.86
0.10	10.19	11.3	3.27
0.15	15.63	13.37	4.62
0.20	24.38	16.25	6.2
0.25	33.2	18.76	9.83
0.30	39.27	24.89	11.22

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 January 2020 doi:10.20944/preprints202001.0303.v1

Table 9 FPR (in %) of various frameworks with varying degree of malicious nodes.

Misbehaving thing ratio	FPR (%)		
	IRAD	*REATO*	*LSFA – IoT*
0	8.3	9.25	2.42
0.05	10.31	12.24	3.65
0.10	19.05	19.01	5.41
0.15	27	23.35	6.57
0.20	34.38	28.62	9.63
0.25	47.6	31.88	11.97
0.30	52.67	39.09	13.83

Table 10 PDR (in %) of various frameworks with varying degree of malicious nodes.

Misbehaving thing ratio	PDR (%)		
	IRAD	*REATO*	*LSFA – IoT*
0	84.4	86.4	98.7
0.05	76.1	80.1	95.4
0.10	70.1	73.1	93.1
0.15	62.3	68.3	90.2
0.20	55.13	60.13	87.1
0.25	49.2	53.2	84.3
0.30	35.23	45.23	81.2

Average values of all methods for all metrics under flooding attack are shown Table 11.

Table 11 Average values of various frameworks for all metrics under flooding attack.

Schemes		*Detection rate*	*FNR*	*FPR*	*PDR*
IRAD	Number of IoT (10% of overall nodes)	63.86	31.058	21.14	72.916
	Number of IoT (20% of overall nodes)	64.83	26.394	26.97	65.106
	Number of IoT (30% of overall nodes)	57.134	22.232	29.77	60.299
REATO	Number of IoT (10% of overall nodes)	70.84	27.23	19.04	77.837
	Number of IoT (20% of overall nodes)	67.458	21.749	22.232	69.54
	Number of IoT (30% of overall nodes)	65.91	18.43	26.392	67.227
LSFA – IoT	Number of IoT (10% of overall nodes)	88.819	14.583	12.011	93.28
	Number of IoT (20% of overall nodes)	87.31	11.629	16.13	83.394
	Number of IoT (30% of overall nodes)	83.005	10.305	17.68	76.947

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 January 2020 doi:10.20944/preprints202001.0303.v1

False Positive Rate: Figure 5 displays the comparison between the suggested LSFA-IOT framework and two other methods of statistical-based method and deep learning-based machine learning method. According to the Figure 5(a), by the number of normal Things within the range of 50-500 and increasing the malicious Things rate from 10 to 30%, a slight and moderate growth will exist in the FPR created by the proposed design in comparison with the two other designs. By the number of normal Things and the rate of malicious Things equal to 500 and 10%, respectively, the false positive rate of the suggested design is less than 15%. Nevertheless, this quantity is adjusted to 22% for the REATO and 26% for the IRAD. The suggested design is superior as the result of the fast detecting the malicious Things and removing them through collaboration between normal Things and source things. Moreover, it is superior since the suggested algorithm finds flooding attack and separates them from the IoT network, hence, the FPR occurring by the attacks is reduced. According to Figure 5(b), and (c), LSFA-IOT reduces the FPR by over 27 and 36% compared to REATO and IRAD models, respectively.

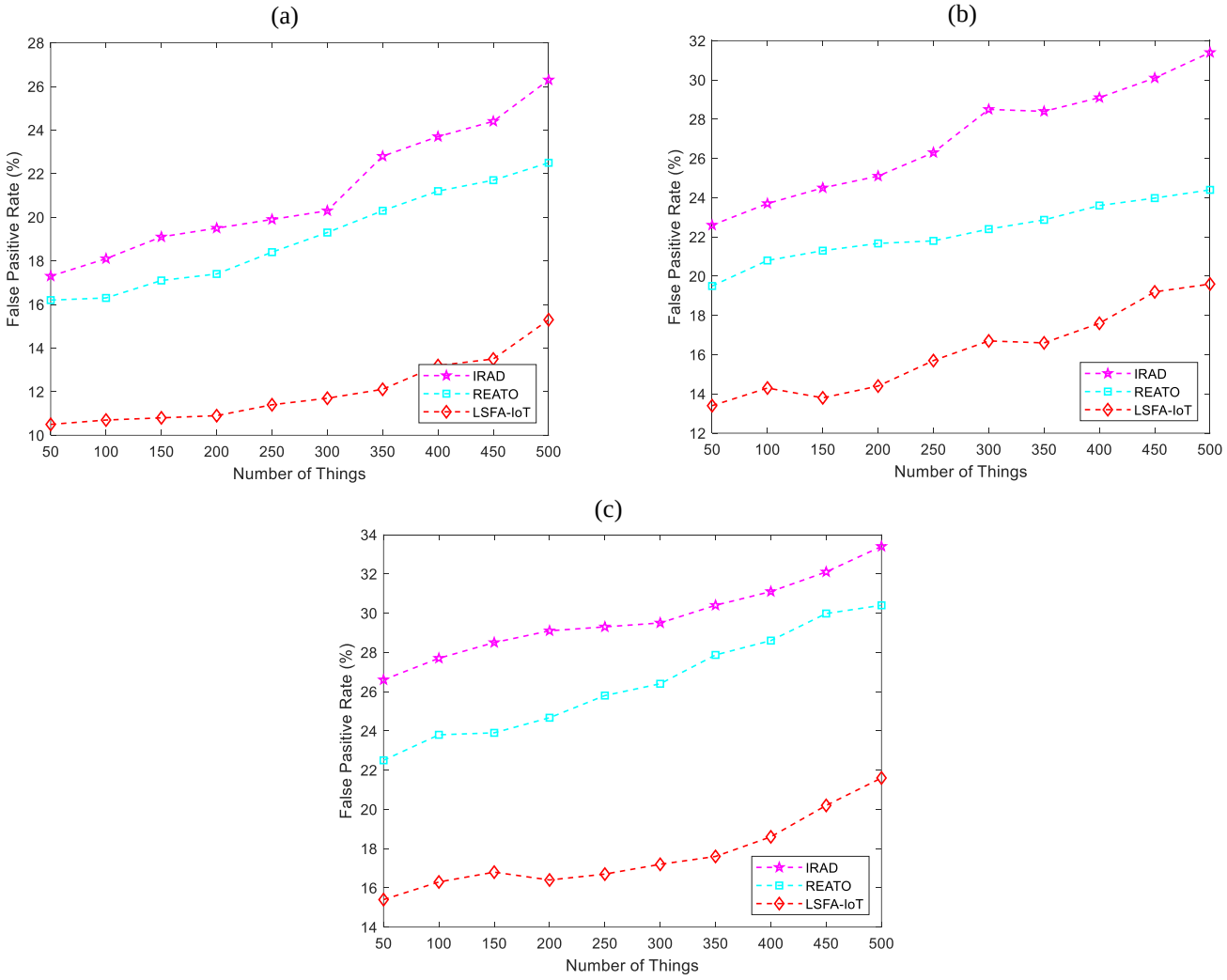


Fig. 5 Comparison of the LSFA-IoT, REATO and IRAD approaches in term of FPR.

False Negative Rate: Figure 6 represents the comparison between the LSFA-IoT suggested scheme, REATO and IRAD models based on FNR in flooding attack. (a) Number of Things (10% malicious), (b) Number of Things (20% malicious), and (c) Number of Things (30% malicious)

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 January 2020 doi:10.20944/preprints202001.0303.v1

respectively. According to the diagrams, there is a slight increase in the LSFA-IoT proposed schema's FNR, however, this value is greater in the REATO and IRAD. In Figure 6(a), the proposed schema's FNR is less than 16% by the number of normal Things as 500, however, it is 32 and 36% respectively for the other two methods. According to Figure 6(b), if the malicious Things rate is 20%, it is less than 12% in the suggested design, although for the other two techniques, this quantity is 25% and 31% respectively. In Figure 6(c), we observe that the adaptation capability of LSFA-IoT is higher than that of other approaches. This superior performance can be attributed to mainly, LSFA-IoT detection scheme.

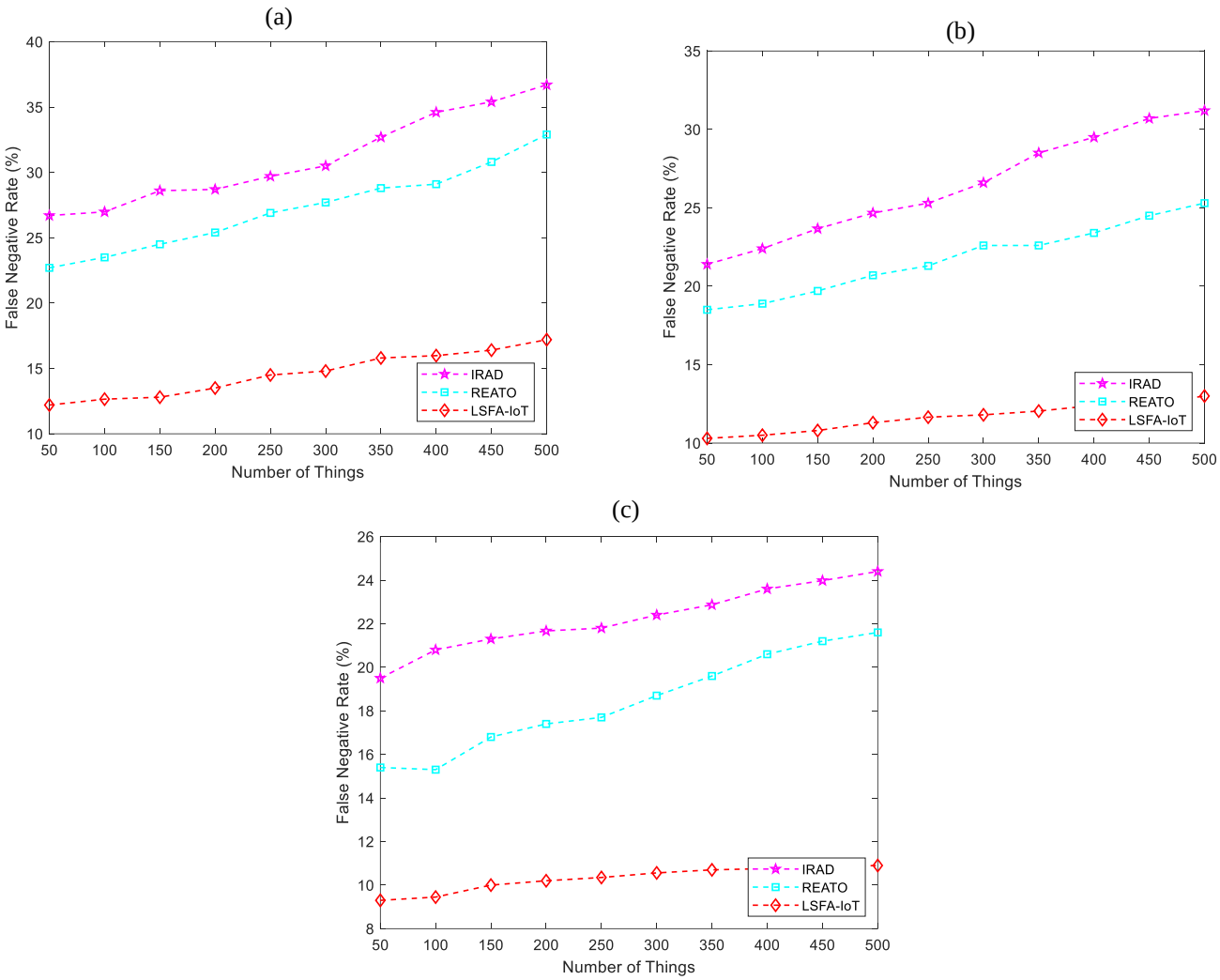


Fig. 6 Comparison of the LSFA-IoT, REATO and IRAD approaches in term of FNR.

Detection Rate: A comparison of the LSFA-IOT proposed scheme, REATO and IRAD models based on DR is provided in Figure 7. (a) Number of Things (10% malicious), (b) Number of Things (20% malicious), and (c) Number of Things (30% malicious) respectively. Based on the diagrams, the detection rate in every three approaches is decreased based on two setups, particularly by the high number of attacks. The decrease is much higher for the REATO compared to the other mechanisms. All the above-mentioned attacks can be detected by the proposed design at a detection rate of over 95%. This finding is obtained when the rate of malicious Things and the number of normal Things are 30% and 600, respectively.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 January 2020 doi:10.20944/preprints202001.0303.v1

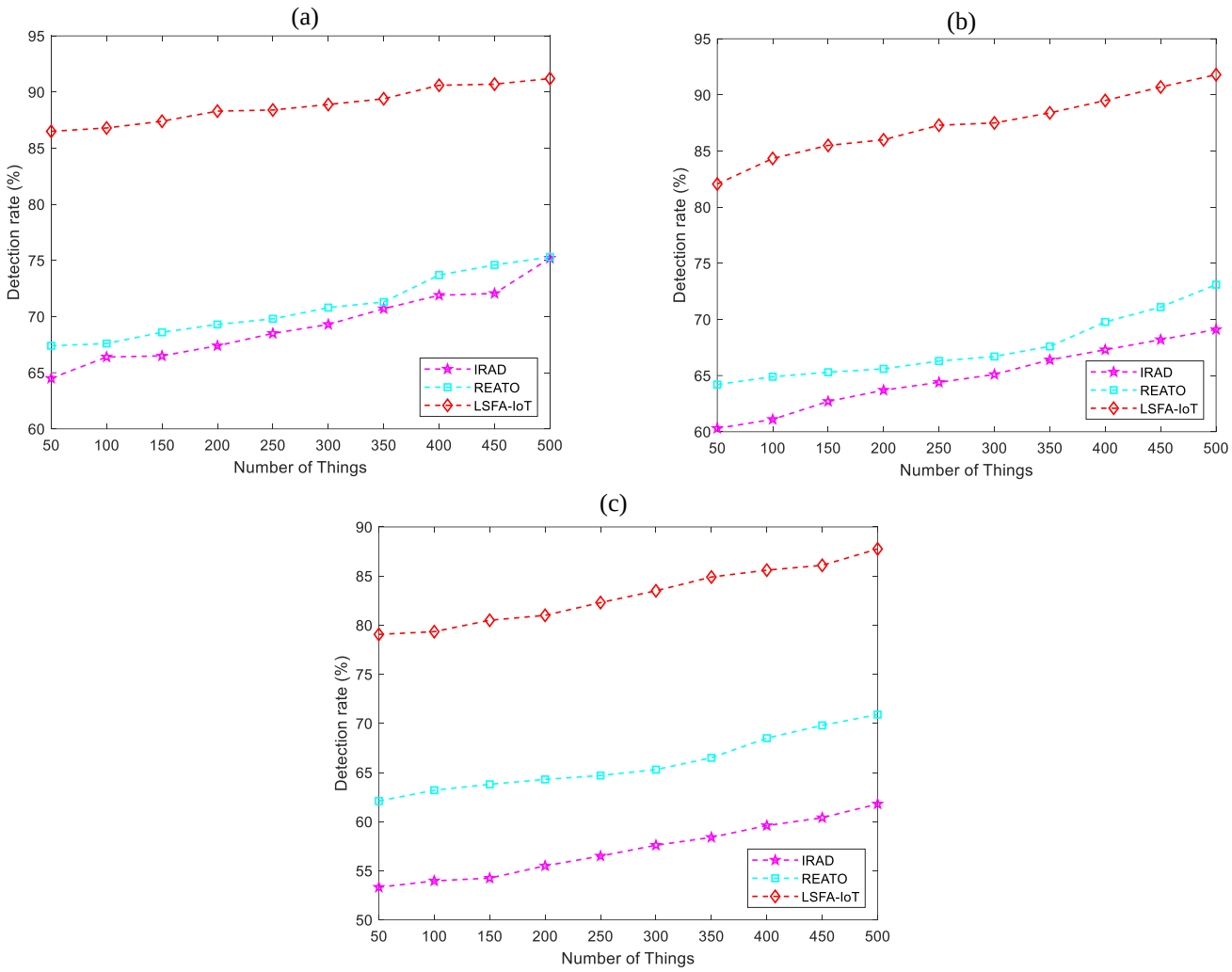


Fig. 7 Comparison of the LSFA-IoT, REATO and IRAD approaches in term of DR.

Figure 8 illustrates the relationship between the packet delivery ratio and the number of Things under the identical setting expressed in Table 5. When the number of Things is 50, we see that some packets cannot arrive themselves to the destination before the timeout period terminates; so, the packet delivery ratios of REATO and IRAD are somewhat low. As the number of Things increases, most packets can be delivered to the destination; hence, we can see a small enhancement in the packet delivery ratios. The packet delivery ratio of LSFA-IoT has an insignificant degradation when the number of Things is 50 and 100. This is due to the presence of random factors in the simulation process. From a general point of view, when the number of Things goes beyond 100-500, LSFA-IoT outdoes both REATO and IRAD in terms of packet delivery ratio. As shown in the Figure 8(a), (b) and (c), LSFA-IoT increases the PDR by more than 22 and 32% those of REATO and IRAD models, respectively.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 January 2020 doi:10.20944/preprints202001.0303.v1

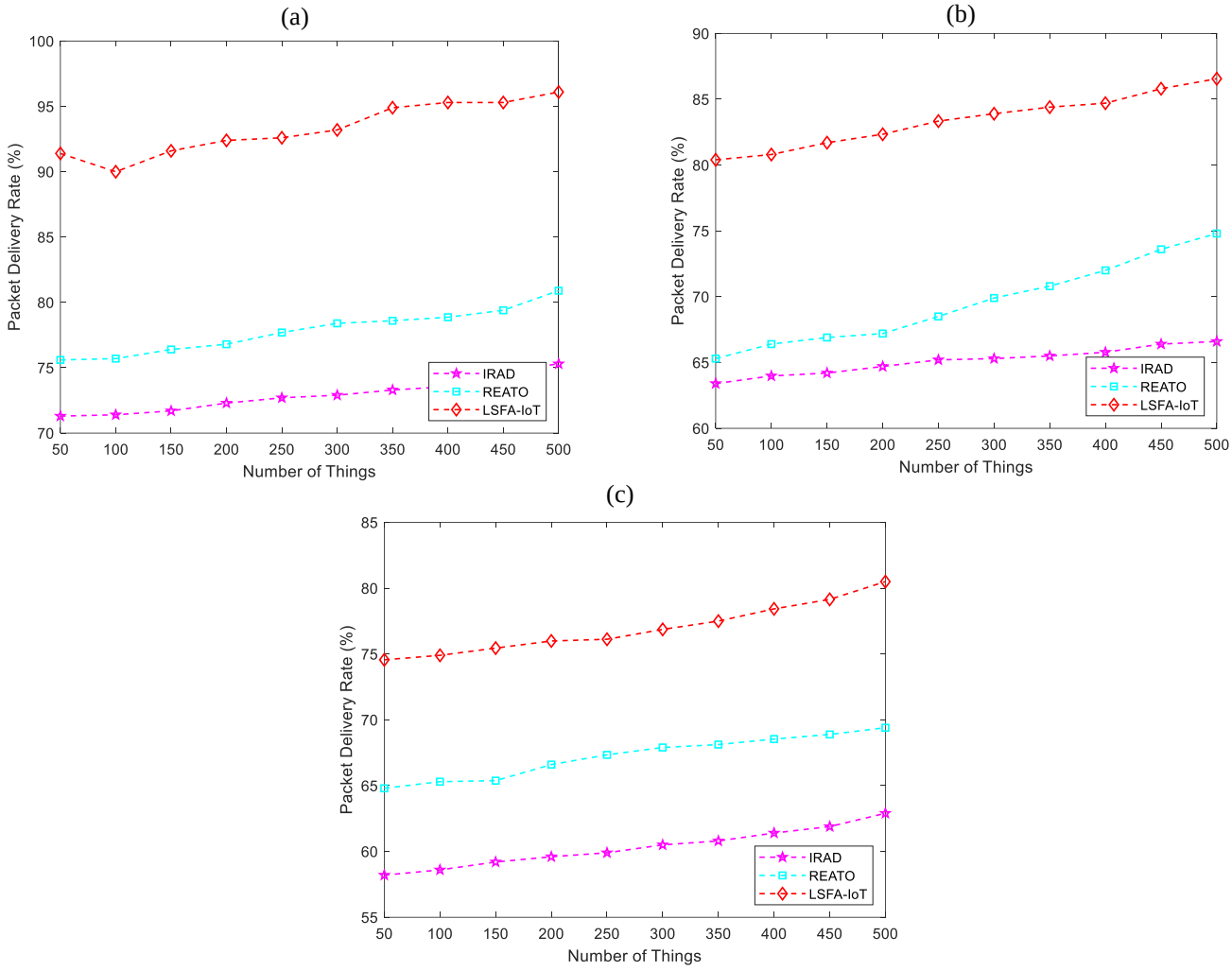


Fig. 8 Comparison of the LSFA-IoT, REATO and IRAD approaches in term of PDR.

6 Conclusion

Increasing the usage of IoT and considering the easy implementation of these networks, these networks are being incremented daily. Hence, to provide protected communications among IoT nodes requires the security necessarily. To overcome the challenges, a secure multi-mode solution is required achieving both vast protected mode and the desired networks' performance. Two key parts are included in the suggested LSFA-IoT schema such as flooding detection system and misbehavior detection system. The first section is utilized for stabilizing the network status. By exceeding the number of route requests the threshold, the nodes become aware of abnormal behavior and misbehavior in the network. The second part is responsible for discovering the misbehavior sources in the network utilizing $APT - RREQ$, the Average Packet Transmission $RREQ$. By detecting a malicious node, the node's status is checked by LSFA-IoT prior to sending a data packet, and in case the node is found as a malicious node, the packet is not sent to that node and the node is added to detention list. The suggested LSFA-IoT can be utilized in effectively managing attacks within the route detection phase and over the data packet transmission phase. LSFA-IOT is more effective than the IRAD and REATO methods under flooding attack since it finds the malicious node previously in addition to

isolating the malicious node and restoring the accused node followed by the penalty period. The main advantage of the LSFA-IOT is that the suspect node can be regarded as a normal node in the network again followed by a rational penalty. Here, we assessed the LSFA-IOT scheme performance utilizing NS-3 and indicated its high level of detection rate and security (more than 91.04%), low FNR (less than 13.33%), low FPR (less than 19.33%), and high PDR (over 88.01%), in comparison with the present techniques.

Conflict of Interest

None.

Reference

1. Zarpelao, B.B., et al., *A survey of intrusion detection in Internet of Things*. Journal of Network and Computer Applications, 2017. **84**: p. 25-37.
2. Fotohi, R., & Jamali, S. (2014). A comprehensive study on defence against wormhole attack methods in mobile Ad hoc networks. International journal of Computer Science & Network Solutions, 2, 37-56.
3. Fotohi, R. (2020). Securing of Unmanned Aerial Systems (UAS) against security threats using human immune system. Reliability Engineering & System Safety, 193, 106675.
4. Fotohi, R.; Nazemi, E. An Agent-Based Self-Protective Method to Secure Communication between UAVs in Unmanned Aerial Vehicle Networks. Preprints 2020, 2020010229 (doi: 10.20944/preprints202001.0229.v1).
5. Mabodi, K., Yusefi, M., Zandiyan, S., Irankhah, L., & Fotohi, R. Multi-level trust-based intelligence schema for securing of internet of things (IoT) against security threats using cryptographic authentication. The Journal of Supercomputing, 1-25.
6. Faghihniya, M.J., S.M. Hosseini, and M. Tahmasebi, *Security upgrade against RREQ flooding attack by using balance index on vehicular ad hoc network.* Wireless Networks, 2017. **23**(6): p. 1863-1874.
7. Pacheco, J. and S. Hariri, *Anomaly behavior analysis for iot sensors.* Transactions on Emerging Telecommunications Technologies, 2018. **29**(4): p. e3188.
8. Zandiyan S, Fotohi R, Koravand M. P-method: Improving AODV routing protocol for against network layer attacks in mobile Ad-Hoc networks. International Journal of Computer Science and Information Security. 2016 Jun 1;14(6):95.
9. Fotohi, R., Heydari, R., & Jamali, S. (2016). A Hybrid routing method for mobile ad-hoc networks. Journal of Advances in Computer Research, 7(3), 93-103.
10. Fotohi, R., & Bari, S. F. (2020). A novel countermeasure technique to protect WSN against denial-of sleep attacks using firefly and Hopfield neural network (HNN) algorithms. The Journal of Supercomputing, 1-27.
11. Fotohi, R., Bari, S. F., & Yusefi, M. (2019). Securing Wireless Sensor Networks Against Denial-of-Sleep Attacks Using RSA Cryptography Algorithm and Interlock Protocol. International Journal of Communication Systems.
12. Chen, K., et al., *Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice.* Journal of Hardware and Systems Security, 2018. **2**(2): p. 97-110.
13. Moon, J., I.Y. Jung, and J.H. Park, *Iot application protection against power analysis attack.* Computers & Electrical Engineering, 2018. **67**: p. 566-578.
14. Jiang, Y., A. Hu, and J. Huang, *A lightweight physical-layer based security strategy for Internet of things.* Cluster Computing, 2018: p. 1-13.
15. Fotohi, R., Ebazadeh, Y., & Geshlag, M. S. (2016). A new approach for improvement security against DoS attacks in vehicular ad-hoc network. International Journal of Advanced Computer Science and Applications, 7(7), 10-16.
16. Behzad, S., Fotohi, R., Balov, J. H., & Rabipour, M. J. (2018). An Artificial Immune Based Approach for Detection and Isolation Misbehavior Attacks in Wireless Networks. JCP, 13(6), 705-720.

17. Behzad, S., Fotohi, R., & Jamali, S. (2013). Improvement over the OLSR routing protocol in mobile Ad Hoc networks by eliminating the unnecessary loops. International Journal of Information Technology and Computer Science (IJITCS), 5(6), 2013.
18. Behzad, S., Fotohi, R., & Dadgar, F. (2015). Defense against the attacks of the black hole, gray hole and wormhole in MANETs based on RTT and PFT. International Journal of Computer Science and Network Solutions (IJCSNS), 3, 89-103.
19. Seyedi, B., & Fotohi, R. NIASHPT: a novel intelligent agent-based strategy using hello packet table (HPT) function for trust Internet of Things. The Journal of Supercomputing, 1-24.
20. Adat, V. and B. Gupta, *Security in Internet of Things: issues, challenges, taxonomy, and architecture.* Telecommunication Systems, 2018. **67**(3): p. 423-441.
21. Alamr, A.A., et al., *A secure ECC-based RFID mutual authentication protocol for internet of things.* The Journal of Supercomputing, 2018. **74**(9): p. 4281-4294.
22. Deng, L., et al., *Mobile network intrusion detection for IoT system based on transfer learning algorithm.* Cluster Computing, 2018: p. 1-16.
23. Bhunia, S.S. and M. Gurusamy. *Dynamic attack detection and mitigation in IoT using SDN*. in *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*. 2017. IEEE.
24. Rostampour, S., et al., *A scalable and lightweight grouping proof protocol for internet of things applications.* The Journal of Supercomputing, 2018. **74**(1): p. 71-86.
25. Lee, S., et al., *Design and implementation of cybersecurity testbed for industrial IoT systems.* The Journal of Supercomputing, 2017: p. 1-15.
26. Qin, T., et al., *IMLADS: Intelligent Maintenance and Lightweight Anomaly Detection System for Internet of Things.* Sensors, 2019. **19**(4): p. 958.
27. Hashemi, S.Y. and F.S. Aliee, *Dynamic and comprehensive trust model for IoT and its integration into RPL.* The Journal of Supercomputing, 2018: p. 1-30.
28. Diro, A.A. and N. Chilamkurti, *Distributed attack detection scheme using deep learning approach for Internet of Things.* Future Generation Computer Systems, 2018. **82**: p. 761-768.
29. Jhaveri, R.H., et al., *Sensitivity analysis of an attack-pattern discovery based trusted routing scheme for mobile ad-hoc networks in industrial IoT.* IEEE Access, 2018. **6**: p. 20085-20103.
30. Jan, M.A., et al., *A payload-based mutual authentication scheme for Internet of Things.* Future Generation Computer Systems, 2019. **92**: p. 1028-1039.
31. Yaseen, Q., et al., *Collusion attacks mitigation in internet of things: a fog based model.* Multimedia Tools and Applications, 2018. **77**(14): p. 18249-18268.
32. Bawany, N.Z., J.A. Shamsi, and K. Salah, *DDoS attack detection and mitigation using SDN: methods, practices, and solutions.* Arabian Journal for Science and Engineering, 2017. **42**(2): p. 425-441.
33. Han, G., et al., *A source location protection protocol based on dynamic routing in WSNs for the Social Internet of Things.* Future Generation Computer Systems, 2018. **82**: p. 689-697.
34. Yan, Q., et al., *A multi-level DDoS mitigation framework for the industrial internet of things.* IEEE Communications Magazine, 2018. **56**(2): p. 30-36.
35. Yavuz, F.Y., D. Ünal, and E. Gül, *Deep learning for detection of routing attacks in the internet of things.* International Journal of Computational Intelligence Systems, 2018. **12**(1): p. 39-58.
36. Sicari, S., et al., *Reato: Reacting to denial of service attacks in the internet of things.* Computer Networks, 2018. **137**: p. 37-48.
37. Fotohi, R., et al., *An Improvement over AODV routing protocol by limiting visited hop count.* International Journal of Information Technology and Computer Science (IJITCS), 2013. **5**(9): p. 87-93.
38. Jamali, S. and R. Fotohi, *DAWA: Defending against wormhole attack in MANETs by using fuzzy logic and artificial immune system.* the Journal of Supercomputing, 2017. **73**(12): p. 5173-5196.
39. Jamali, S. and R. Fotohi, *Defending against wormhole attack in MANET using an artificial immune system.* New Review of Information Networking, 2016. **21**(2): p. 79-100.
40. Jamali, S., Fotohi, R., Analoui, M. (2018). An Artificial Immune System based Method for Defense against Wormhole Attack in Mobile Adhoc Networks. TABRIZ JOURNAL OF ELECTRICAL ENGINEERING, 47(4), 1407-1419.
41. Sarkohaki, F., R. Fotohi, and V. Ashrafian, *An efficient routing protocol in mobile ad-hoc networks by using artificial immune system.* International Journal of Advanced Computer Science and Applications (IJACSA), 8 (4), 2017.