A trust management scheme to secure mobile information centric networks

Rathee, G., Sharma, A., Kumar, R., Ahmad, F. & Iqbal, R.

Original citation & hyperlink:
Rathee, G, Sharma, A, Kumar, R, Ahmad, F & Iqbal, R 2020, 'A trust management scheme to secure mobile information centric networks', Computer Communications, vol. 151, pp. 66-75.
https://dx.doi.org/10.1016/j.comcom.2019.12.024

DOI 10.1016/j.comcom.2019.12.024
ISSN 0140-3664

Publisher: Elsevier

A Trust Management Scheme to Secure Mobile Information Centric Networks

Geetanjali Rathee[a], Ashutosh Sharma[b,*], Rajiv Kumar[c], Farhan Ahmad[d], Razi Iqbal[e]

[a] *Department of Computer Science and Engineering Jaypee University of Information Technology, Waknaghat-173234, Solan, India, geetanjali.rathee123@gmail.com*
[b] *Department of Electronics and Communication Engineering, Lovely Professional University, Phagwara - 144402, Punjab, India, sharmaashutosh1326@gmail.com*
[c] *Department of Electronics and Communication, Jaypee University of Information Technology, Waknaghat-173234, Solan, India,rjv.ece@gmail.com*
[d] *Cyber Security Research Group, College of Engineering and Technology, University of Derby, United Kingdom, f.ahmad@derby.ac.uk*
[e] *Al-Khawarizmi Institute of Computer Science, University of Engineering and Technology, Lahore, Pakistan, 50400, razi.iqbal@ieee.org*

Abstract

The Named Data Networks (NDN) or Information Centric Networks (ICN) are being replaced by point-point procedures in order to ensure a reliable and efficient communication mechanism.The efficient benefits of ICN in terms of improved reliability, efficiency and fast information delivery lifted it as a highly capable interconnected networking form for Internet infrastructure. Smart devices in Mobile Internet of Things (MIoT) and ICN contribute towards exponential growth of technical firms by ensuring reliability, efficiency and availability. Though NDN architectures ensure a secure data communication, however, in order to gain their own benefits, the expert intruders may compromise routers (nodes) and their routing tables. Therefore, in order to ensure a secure communication through MIoT, any modification in stored data of these devices (routers) must be transparently reflected to remaining entities in the network. Recently, trust is proposed as an alternative security measure to secure content delivery within ICN. However, only few of these solutions focused on identifying the legitimacy of the devices. In this paper, we proposed a novel ICN approach to compute the legitimacy

[*] Corresponding author

of MIoT devices/routers/nodes and routing paths information using trust based on a wide range of real-life parameters including energy consumption while transferring the data from source to destination, message delivery to preceding or succeeding nodes and distance among two devices to identify Denial of Service (DoS), Distributed Denial of Service (DDoS) or Man-in-The-Middle (MiTM) attacks. The proposed solution is evaluated rigorously over various networking parameters such as distance among the devices, energy consumption, information loss while transferring the data and so on. Further, the extensive simulation results of proposed mechanism leads to 94% efficiency in terms of better response time, lower authentication delays and request ratios from fake nodes.

Keywords: IoT devices, Mobile Internet of Things, Named Data Networking, Information Centric Networking, Trust model

1. Introduction

New frontiers of technologies and machines have been incorporated to ease and improve the daily life of human beings. IoT is one such technological front that aims to connect various devices into a common network. For its applications in ambulant environments like smart cities and vehicular networks, it has been further modified into Mobile Internet of things (MIoT) which incorporates the mobile nature of the devices. The goal of MIoT is to provide a connection to the users from anywhere and at anytime which makes it an attractive mechanism in research and industrial sectors [1]. While IoT is an umbrella term used to denote a network of devices, MIoT is a type of IoT in which the devices are mobile in nature instead of being static. A network of vehicular devices may be considered as an IoT network but it can also be called as an MIoT network with more specificity as the devices are mobile.

Another efficient mechanism to further improve communication and networking is Information-Centric Networking (ICN), an approach that aims to evolve the internet infrastructure from host-centric to data-centric prototype [2]. The efficient benefits of ICN in terms of improved reliability, efficiency and fast information delivery lifted it as a highly capable networking form for MIoT [3]. The world has entered in the era of automated and wearable devices loaded with sensors where the information gathered from the environment is relayed to remote location for auxiliary analysis. In order to ensure an efficient and reliable communication among various entities, point-to-point communication procedure has been replaced by one of the ICN architectures known as 'Named Data Networking (NDN)' [4]. This architecture further improves the data-centric approach by emphasising on content rather than its location. In spite of heterogeneity, scalability and dynamicity, internet protocol is still the most widely used solution in the prospects of NDN.

NDN is a prospective networking approach that has been inspired by long term future centric research to solve various contemporary problems associated with the current IP architecture [5]. The main proposition of NDN is that the data should directly be accessed by the users and not via a named host or client framework. It include various data structures to ensure that all the numerically addressed hosts are replaced by named data where IP architecture being non-generic in nature fails to constitute any protocol stack other than the TCP/IP suite. Further, the security of data is a major concern with the existing IP mechanism. The intruders may disrupt the IP address and introduce various security threats in the network such as reliability, denial-of-service and unavailability of services. ICN does not transmit data using these IP addresses and therefore identification of packets in transit is almost impossible. In addition, NDN is a data-centric framework where only sender and receiver knows which data needs to be reconstructed and hence this provides an additional layer of security over the encryption technique [6].

NDN can be used by corporations that want a secure method of sending and sharing data and float a data request without revealing the host entity. In today's era of smart technological devices, NDN provides a new space for organizations to efficiently manage and send data. Smart devices i.e. IoT enabled devices also have a significant contribute towards this exponential growth of technical firms by ensuring reliability, efficiency and availability. Suppose a device connects to the internet after entering an established IoT network. The node may use NDN and data-centric approach over the internet and may broadcast its request to the various parties on the internet but the communication will remain hidden from other devices in the network which may also connect to the internet on an individual level.

1.1. Motivation and Contribution

In spite of a wide range of advantages offered by IoT technology, MIoT objects applied using NDN technology may still be adversely affected in a number of ways. Providing a secure mechanism for MIoT devices is not only important for the NDN technology but also for various other mechanisms that use IoT devices. Although, NDN-MIoT mechanism leads to a secure framework for ensuring a safe data message transmission using various cryptographic mechanisms. However, other data structures such as routing paths' information in ICN may still be compromised by the intruders with the intent of degrading the network performance in various aspects. The distributed and scalable features of IoT can be exploited by the attackers by encountering various Denial of Service (DoS) and Man-in-Middle (MiTM) attacks. Denial of Service (DoS) is a cyber attack in which the intruder attempts to make a device temporarily unavailable with the intent of disrupting the communication process. Further, the Distributed Denial of Service (DDoS) is a specific type of DoS attack. In DDoS, a malicious attempt is made by the intruders to disrupt normal functioning by flooding the devices with internet traffic. Both DoS and DDoS are highly menacing and unpredictable attacks to the NDN-MIoT [7, 8].

To address above issues, trust management can be introduced in the network with the aim to provide security to the IoT devices. Therefore, the sensors or nodes that provide the services to their respective users (entities) must be recorded and analyzed regularly to check their behaviour in the network. Now a days, various cryptographic solutions have been developed in order to provide content delivery for MIoT devices within network structures like ICN. However, these solutions fail to provide desired results during the data transmission over the network with respect to high energy consumption, communication losses, low resource utilization, untrusted routing path and high key management overhead etc [9, 10, 11]. Therefore, to address these issues, we have introduced a trust based approach that ensures the transmission of trusted content over the network [12]. The proposed mechanism has been validated over various metrics including user's request response, utilization of resources, response time, number of processed request, probability of attack detection and success rate, authentication delay, end-to-end delay and throughput, DoS and DDoS attacks. The main contributions of this research study are summarized below:

1. A novel trust management scheme to secure MIoT devices for NDN networking approaches is proposed to evaluate the trustworthiness of the legitimate nodes that provide the data to the communicating or routing processing entities within the MIoT.
2. The legitimacy of each MIoT device is identified by computing the trust

value depending upon a wide range of parameters including authentication delay, response time, probability of attack detection, end-to-end delay and throughput, to name a few.

3. Further, Johnson's algorithm is used within NDN for finding the shortest path routing algorithm to speed up the communication process among the devices in real-time scenarios.
4. Finally, extensive simulations are carried out to validate our data-centric proposal for securing the MIoT.

The rest of the manuscript is structured as follows. The survey of literature related to ICN and MIoT devices from trust and security perspective is presented in Section II. The proposed trust framework for MIoT is described in Section III. Further, Section IV analyzes the performance metrics of the proposed scheme against various security networking metrics such as response time, authentication delay and request ratio. Finally, Section V concludes the work and highlights the future recommendations for this work.

2. Related Work

2.1. MIoT in Named Data Networking

The security of MIoT devices is critical for an efficient and reliable communication process. The use of NDN in MIoT architecture resolves a number of contemporary issues such as privacy preservation. To resolve the various problems of existing networking architectures, NDN allows the direct access of data by the users and drives the communication process in two ways to exchange the data from source to destination, i.e., via *interest* and *data* packet type. *Interest* packet is the one where information is forwarded by integrating the desired data name into an interest packet whereas in *data* packet type, interest reaches the requested data node by putting both content and name along with the producer's signature [13]. To further carry out the data packet forwarding and interest functions, each data network maintains three types of data structures i.e. Pending Interest Table (PIT), Forwarding Information Base (FIB) and Content Store (CS) [14]. PIT stores all the interest forwarded by the router that are not yet verified in the network. Each PIT contains the data name carried in interest along with its incoming and outgoing interfaces. Further FIB maintains a routing table that directly maps the name to interface and finally CS where a cache is used to temporarily store the data packets. Among these data structures, the security issues in PIT and FIB structures are of more concern. While keeping the record of each router and accessing the information of named data through routing tables, NDN architecture ensures a secure delivery of data by requiring the cryptographic signature of every data packet. Though NDN ensures secure delivery of data packets among the nodes or routers, however, the advanced security concerns such as compromised MIoT nodes or routers may lead to security issue within the MIoT networks. Even though the data is secured in the network, the compromised MIoT devices lead to drastic degradation of the communication and transmission process in the network. Therefore, in order to inflict cooperation among communicating entities and isolate the malicious MIoT devices, this paper has proposed a secure trust mechanism that considers the PIT and FIB structures to eliminate communication attacks during message transmission or during path searching process by computing the trust of each MIoT device. This section illustrates the hierarchical ICN architecture along with a rival model to portray the designing methodology and the proposed approach.

NDN offers an intrinsic security as data itself is secured by signing of each information by individual producers. Figure 1 depicts the vanilla architecture of NDN [15] where data packets are hierarchically verified for authentication upon receiving from an author 'P' and published in a blog 'JUIT'. The authentication of the data packet is carried out in three different steps i.e. 1) verification of the signature of the author 'P', followed by 2) checking the blog administrator signature which certified 'P' and finally, 3) verification of the authority which certified the blog administrator. The complete verification process of proposed mechanism resulted in the generation of an authentic data packet. In the next section, we identified various security schemes presented in literature to secure IoT via traditional ICN and NDN.

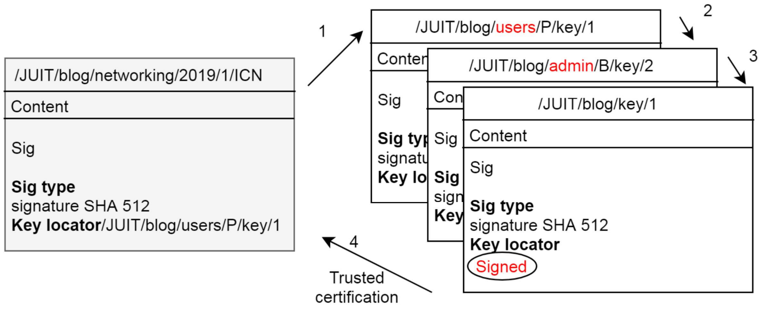

Figure 1: NDN Vanilla architecture

2.2. Literature Survey

Nour et al. [16] have illustrated the benefits of NDN in IoT networks by using content as a fundamental element that can be redistributed and cached. Further, the authors have highlighted the privacy and security challenges in NDN. However, the routing threats occurred during communication procedure is missing from this study. Furthermore, Nour et al. [17] presented the limitations and challenges of NDN as publisher-subscriber by proposing a group-based architecture. The proposed mechanism efficiently provided access control, authentication and group management features without altering the traditional NDN principles. The proposed mechanism is validated against conventional policy-based subscription that showed improved privacy and security features. However, the security issues occurred during packet transmission process is not identified by the authors. Next, Zhang et al. [18] have discussed the advantages of NDN architecture that changed the packet delivery process from IP address hosts to named retrieval of secured data packets. Further, NDN have changed the network security approach that uses name semantics to use cryptographic keys for ensuring the security. In this article, the authors have proposed availability, confidentiality, data authentication and bootstrapping for securing the transmitted data packets within the network.

However, in order to make a practical use, there is a need to address the content security issues of NDN architecture. For instance, Yu et al. [19] have proposed a digital signature scheme using network coding, privacy preserving, post quantum and cost effective signatures to achieve authentication and data integrity in variety of NDN applications. The authors suggested various techniques to speed up the process to ensure signature verification and generation in time. However, the signature verification and generation process at each node further leads to increased computational overhead. Moreover, the proposed mechanism investigated the number of trusted schemes that need certificate less security mechanisms. Next, Rezende et al. [20] have proposed a key management mechanism for reducing the overhead and ensuring a secure data model in NDN. The authors have proposed a replication based scheme to disseminate the status of key by improving the robustness, key status availability and convergence time metrics throughout the communication process. The proposed phenomenon is validated against original data producer which identified a significant reduction in consulting the key status of response time. Further, Zhang et al. [21] have proposed a trusted NDN mechanism for ensuring authenticity, integrity and Provence by managing certificates and cryptographic keys in a meaning full manner. The proposed mechanism provided the trust among two entities or within a single entity by generating a certificate using its name space. However, they have not considered further security issues concerned to NDN architecture. Tschudin et al. [22] have proposed a logical trust engine for NDN which is capable of correctly and efficiently verifying the authenticity and integrity of data. This trust engine is implemented in CCNx stack to further validate the availability of the network. Yu et al. [23] have proposed a secure NDN architecture that ensures data authentication to sign and verify each data packet in the network layer. In order to make authentication decision usable through a trust-based scheme that defines which key may sign which data and verification procedure. The authors have proposed a trust model to handle the key generation and verification procedure during data authentication. NDN with internet have introduced the future internet architecture by offering a multicast, in-network caching, mobility and security through content-based communication. In this article, Nour et al. [24] have illustrated a systematic and detailed review of IoT-ICN where ICN enables communication for benefiting the IoT networks. In addition, the authors have surveyed Quality of Service (QoS), interoperability, mobility, security challenges and research directions.

Aboodi et al. [25] have discussed the issues of incorporating NDN architecture with IoT in terms of access control, naming schemes for data and devices, forwarding strategies, in-network caching and device configurations. Mick et al. [26], on the other hand, have proposed a scalable and novel security framework for hierarchical and lightweight authentication in NDN. The authors have highlighted the new routing and on boarding security challenges in NDN based IoT networks. The NS3 based simulation validated the efficiency and scalability of the proposed phenomenon for large scale IoT applications as in smart cities. In order to improve efficiency and throughput in 5G IoT application, Lei et al. [27] have proposed a probability-based forwarding strategy for network coding. For quantifying the performance benefits, authors have used ndnSIM simulator by integrating NDN into network coding. The experimental results demonstrated the significant improvement of QoS, reliability and performance. Zhu et al. [28] have addressed the security challenges of NDN-IoT architectures and analyzed the impact of network performance against several security attacks. Lastly, a blockchain-based solution is provided against NDN-IoT security threats.

Although there are various security improvements in NDN, yet there have been numerous setbacks. Various threats such as compromising the nodes and intrusion of the routing path mainly via DoS, Man-in-middle and black hole attacks are still persistent. Active research is going on in this domain, where many studies have relied on cryptographic techniques to ensure security within NDN. However, cryptographic solutions offer various limitations due to their complex nature with respect to communication, computation, key management and storage overheads. Therefore there is strong need for an efficient security mechanism for the MIoT network. The goal of this paper is to achieve an efficient NDN-enabled environment by securing the MIoT devices that comprise this novel paradigm.

2.3. Existing Approach

In order to validate the proposed phenomenon, in this paper, an NDN framework is compared against a recent trusted model proposed by Fang et al. [29]. They have proposed a trusted model that have discussed the need of cyber security by analyzing typical threat behaviours and defence mechanisms. In this study, the authors proposed an efficient trust-based solution to resolve an intelligent internal on-off threat. Simulation results proved the efficiency of this solution by identifying and revoking malicious devices from the network in a short span of time. The author's computed the network trust via two different methods i.e., directly and indirectly, solely depending upon their reputation within the network. Further, trust is analyzed based upon its data transmission and the information is updated accordingly. However, in our proposed phenomenon the accuracy of nodes trust or legitimacy is enhanced by calculating the weights using trust weights. Further, The value of trust increments and decrements based on various networking parameters such as energy consumption, previous interaction and information loss etc. The simulated results of proposed framework shows better results against various measuring parameters such as accuracy of service response during the involvement of malicious activities by the intruders, response time by the IoT devices in malevolent environment, efficient utilization of resources where some of nodes are compromised by the attacker and finally the number of processed request by the devices sent by various users. All these measuring parameters are efficiently compared and analyzed against exiting (traditional) approach.

3. Proposed Solution

The NDN is assumed to be hierarchical in nature. In this paper, we categorized the NDN architecture into three distinct layers, i.e., (1) End user layer, (2) IoT sensor layer, and (3) Internet layer. The end user layer constitutes the lowest layer of the architecture which include healthcare systems, industries, cities and cab services. Next layer is the IoT sensor layer which consists of IoT devices (known as sensors) are allied above the end users. Further, Internet layer is the top most layer of proposed architecture through which the services are provided to IoT sensors. The generic network model of the proposed framework is depicted in Figure 2 with an assumption that the network may drop, duplicate and selectively broadcast the information at anytime, anywhere in the network. The depicted Figure 2 contains number of IoT devices/sensors that can be adopted for vehicular networks, smart cities, smart industries (industry 4.0) and smart healthcare applications, to name a few. However, attacks from various intruders during the communication process with the aim of forging the legitimate device's address and consuming the resources for their own benefits is a major concern in NDN networks.

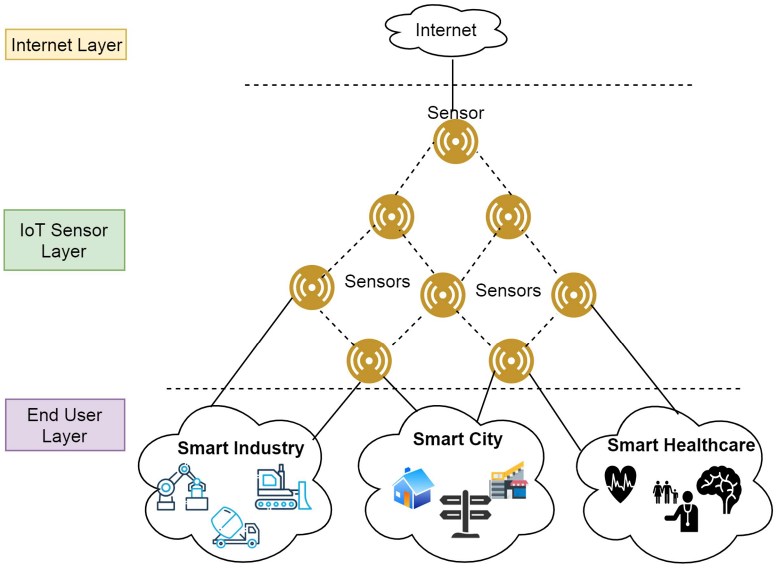

Figure 2: Hierarchical architecture of network model

Moreover, the compromised devices may also indulge in various illegal or unethical deeds such as path information modification and non-optimal route range during communication process to launch various threats inside the network such as worm hole attack, Sybil attack etc. In this paper, we have focused on some major threats which are considered as the most severe attacks of IoT devices in NDN and other mechanisms for causing significant packet drops, delays and degradation of the network performance [30]. The proposed trust framework is evaluated over all the attacks as mentioned below:

- *Black-hole attack:* is the one where the malicious device attracts all the remaining legitimate nodes by promising the shortest path to destination,
- *Data-falsification attack:* during this attack the devices involved in communication transmit false information to the corresponding network.
- *DoS attack:* is a cyber attack in which the intruder attempts to make a device temporarily unavailable with the intent of disrupting the communication process.
- *DDoS attack:* the Distributed Denial of Service (DDoS) which is a specific type of DoS attack and a malicious attempt to disrupt the normal functioning by flooding the devices with internet traffic is also highly menacing and unpredictable to the NDN-MIoT.
- *Man-in-the-Middle attack*, during this attack the attacker secretly alters the communication between two parties who believe that they are in direct communication with each other.

3.1. Proposed Generic and Adversary Model

By considering these attacks, an adversary model is also depicted in Figure 3. The adversary model includes a number of threats where sensors that provide services to various firms can be easily compromised by the intruders for their own benefits. The attacking devices show-up during the communication process and start behaving as legitimate devices by forging legitimate identity. In order to ensure the entire communication process where devices may freely provide secure services to their requested users in various firms, there is a need to propose a secure communication mechanism. In this paper, we proposed a trust framework to secure MIoT devices for NDN environment based on weight computation. The next section provide details of the proposed trust solution within NDN.

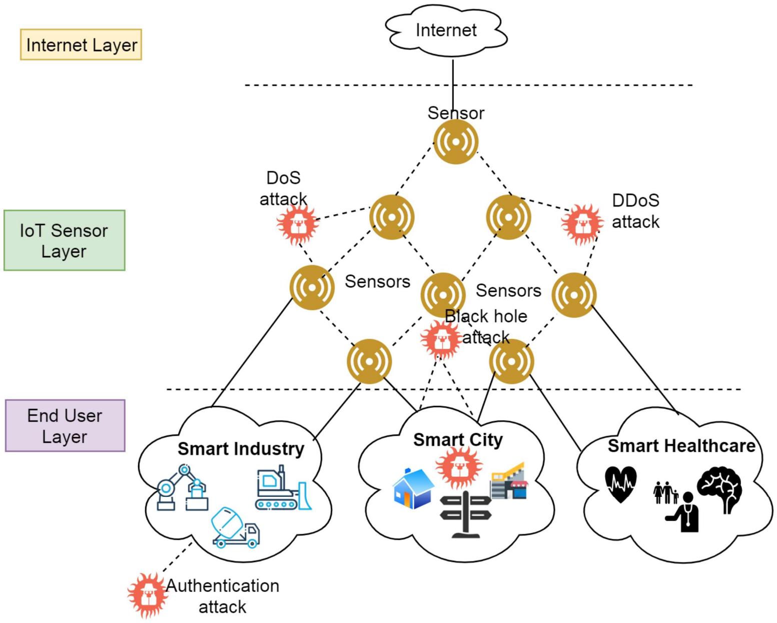

Figure 3: Hierarchical architecture of adversary network model

3.2. *Proposed Trusted Scheme*

The whole scheme is composed of four parameters as listed below which have been elaborated in the following subsections.

1. Route Selection.
2. Weight Computation.
3. Trust Negation.
4. Path Selection.

3.2.1. *Route Selection*

The first main component of our proposed trust management scheme is the route selection for the data generated by the IoT devices from source towards destination. In order to do so, we relied on Johnson's algorithm, which computes the shortest route for the packets generated from source X

to destination Z [31]. Johnson is the shortest path routing algorithm and is used in this paper because of its high speed for searching the communicating path in hierarchical environment. Further, in order to securely broadcast the information among X and Z, the trust of each device that is based upon former interactions and the weight of each device to search shortest route are premeditated using certain metrics. The remaining text argues the basic design of each parameter that is used to route, secure and broadcast all information among communicating entities. The proposed scheme uses preceding history interaction (PHI) for the trust computation of each device because it helps in easy detection of malicious nodes from a database of their preceding activities. Further, a route discovery between source and destination is projected using Johnson's algorithm by computing the weights.

3.2.2. Weight Computation of Nodes

In order to use Johnson's algorithm, each IoT device must consign some weights to calculate shortest route between X and Z. The weights used for searching and communicating the path are calculated via various metrics such as (1) distance between devices, (2) device trust, (3) energy consumption and (4) information delivery rate.

To compute nodes' weight, we first calculate the Euclidean distance $ED_{(i,j)}$ between d_i and d_j using

$$ED_{(i,j)} = \sqrt{((x_i - x_j)^2) + ((y_i - y_j)^2)} \tag{1}$$

where i, j are the network devices and x and y are their coordinates in the network.

Once, $ED_{(i,j)}$ is identified, the next phase of our proposal computes device trust which is achieved via PHI. PHI states that the trust of a sensor known depends on the history of preceding communications by assigning a rank to each device by checking their energy consumption and packet information in the network. Initially, each device is assigned a static trust value let say 0.5 ranging from 0.5 - 1 which can be further decreased and increased by computing the rank of each device using predefined assumed threshold value.The trust value 1 is the highest value. The trust measured from 0.5 - 1 can be further varied according to opinions provided by neighbours. The reason of assuming this range is that threshold will be 20% of maximum, so that taking initial range will help in the further computation instead of considering every value as simply 1. The limitation of taking these initials is that few devices tend to lose the trust as compared to other devices. The formula for computing trust is defined as:

$$Device\ trust = \sum_{i=1}^{n} PHI\ where\ n\ are\ the\ number\ of\ IoT\ devices \tag{2}$$

Further, energy consumption (EC) is the energy consumed by the device that is measured after broadcasting the information. Here, device energy is consumed upon each sending and receiving of information and is measured for weight computation.

$$EC = Total\ energy\ -\ (E_c\ +\ E_r) \tag{3}$$

where E_c is the energy lost during information communication and E_r is energy worn out during receiving of the packets. Finally, information delivery rate decreases due to internal threats on the device that are compromised by the intruders. The device weight (w_n) is defined as sum of consumed energy, information loss (IL means the number of packets or messages lost by the nodes during communication mechanism) and distance between the devices multiplied by some common factor and negation of trust given as:

$$w_n = \sum_{i=1}^{n}((\alpha\ \times\ EC\ ) + (\ \alpha\ \times\ IL)\ + (\alpha\ \times\ d_{(i,j)})\ +\ (1 - trust) \tag{4}$$

The weight calculation and routing mechanism is explained in detail in a flowchart of proposed approach as depicted in Figure 4. In the given flowchart, an initial trust is assigned randomly to all the nodes that can be further increased or decreased depending upon certain communicating factors. The resulting weights computes the overall trust value which ultimately decides the legitimacy of IoT devices.

3.2.3. Significance of Trust Negation

Let us suppose, the communicating routes to broadcast the information to destination Z as given as i-z and j-z with the assumption that trust of the device i is 0.7 and j is 1. Now, according to PHI, the device having maximum trust would be certain to route information. Initially, all the parameters to

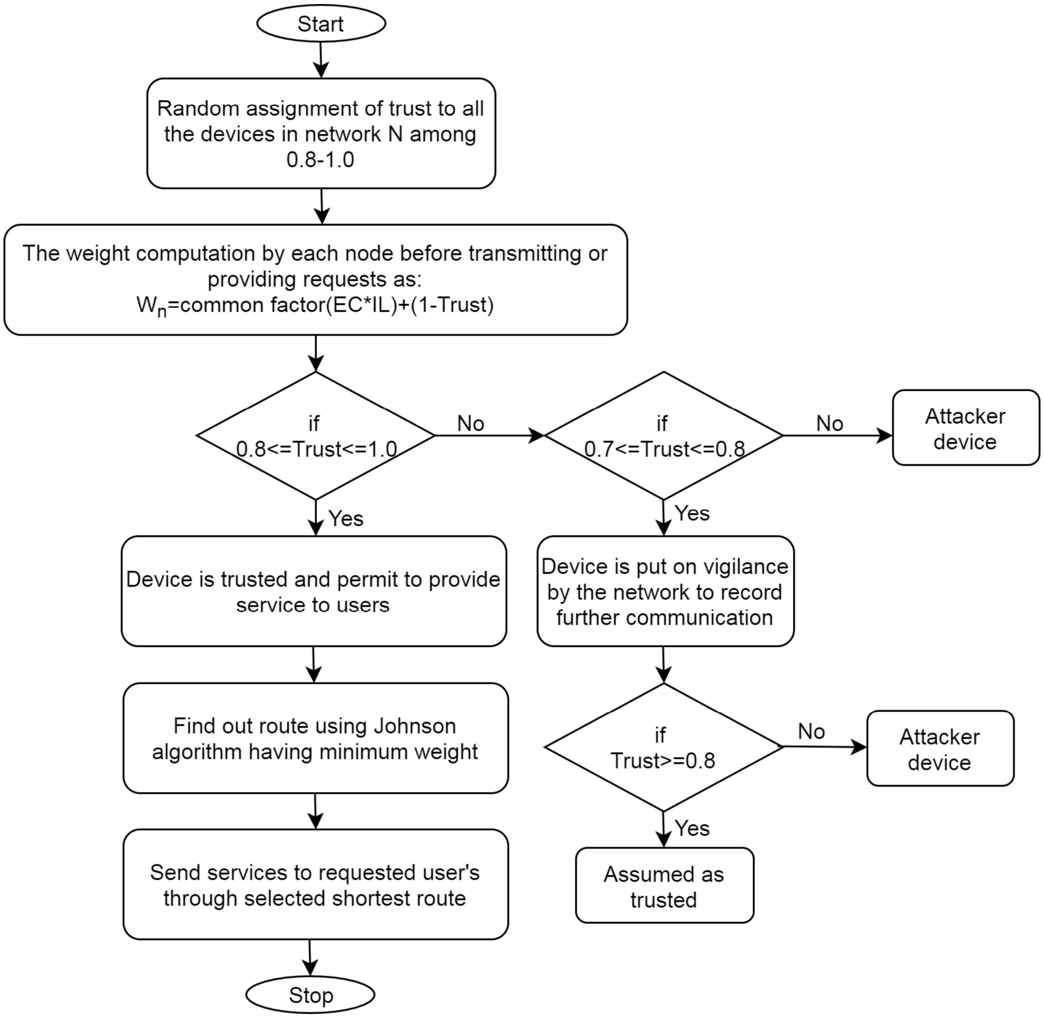
Start
Random assignment of trust to all the devices in network N among 0.8-1.0
The weight computation by each node before transmitting or providing requests as:
W$_n$=common factor(EC*IL)+(1-Trust)
if 0.8<=Trust<=1.0
No
if 0.7<=Trust<=0.8
No
Attacker device
Yes
Yes
Device is trusted and permit to provide service to users
Device is put on vigilance by the network to record further communication
Find out route using Johnson algorithm having minimum weight
if Trust>=0.8
No
Attacker device
Yes
Send services to requested user's through selected shortest route
Assumed as trusted
Stop

Figure 4: Flowchart of proposed trusted architecture

compute the weights are set to be 1 where the corresponding weights of i (w_{i-z}) and j (w_{j-z}) will be computed according to eq. 5 and eq. 6 as follows:

$$w_{i-z} = 0.2\times 1 + 0.2\times 1 + 0.1\times 1 + (1-0.8) = 0.2+0.2+0.1+0.2 = 0.7 \quad (5)$$

$$w_{j-z} = 0.2\times 1 + 0.2\times 1 + 0.1\times 1 + (1-0.9) = 0.2+0.2+0.1+0.1 = 0.6 \quad (6)$$

The weight of device d_{iz} is 0.7 while that of device d_{jz} is 0.6, therefore, route selection by X would be through d_{jz}. The higher is the trust value, the lesser would be the weight. In this way, the device having trust less than weight would be chosen for route formation process.

3.2.4. Path selection

To search a path in NDN networks, Johnson algorithm is used that works on positive weights and is based upon Dijkstra's that searches the minimum weighted routes starting from X and generates a tree till Z. Now, according to PHI, threshold value such as 0.7 is set to each device so that if PHI of any device is less than the threshold than trust would be less and would never be considered for path formation. Similarly, if trust is above 0.7, the device would be considered as trusted.

$$Trust = \frac{PHI}{EC + IL + PHI} \quad (7)$$

Moreover, in order to understand the proposed framework, let us assume a scenario as depicted in Figure 5, where initially random trust would be assigned for computing the weight of each device.

The weights of network would be computed through equation (4) where previous trust of the device would be used to search the new weight. Now, assume if a device P desires to forward information to device Q, trust of device Q would be considered for weight calculation as follows:

$$w_{(p,q)} = 0.2\times EC + 0.2\times IL + 0.2\times D_(p,q) + (1-0.96) \quad (8)$$

Let us suppose that EC, IL and $D_{p,q}$ are set to 1 then the corresponding weights would be computed through eq.(4) as shown in figure 5(b). Moreover, if X desires to forward some information to destination Z, information will be transmitted by computing the shortest route using Johnson's algorithm among X and Z.

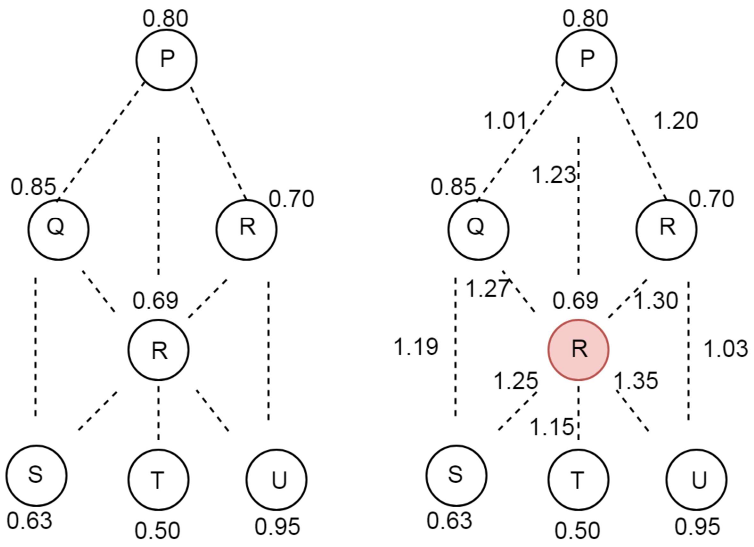

Figure 5: Example of proposed trusted scheme a) trust assignment b) weight calculation

4. Performance Analysis

4.1. System State

In order to overcome the security challenges in MIoT such as while transmitting and routing the data packets, a trusted mechanism is proposed that is further validated and verified through numerical simulations. We imple-

Table 1: Simulation Matrices

Networking Parameters	Values
Simulation time	300 sec
Simulation area	400×400
Networking area	200
No. of IoT devices	50, 100
Mobility model	random
PHY layer	PHY 802.11
MAC protocol	IEEE 802.11
Number of attackers	20, 50 %
Range of transmission	120 m
Size of user's request (number of Packets)	256 Byte

mented and validated our proposed trust mechanism to ensure IoT device security over NS-2 simulator. Although it is a very challenging task to ensure security of every connected IoT device, we have presented a trusted scheme that not only guarantees devices' security but also recommends the services to the real-time environment. In the proposed scheme,the approach is verified against ideal and malicious behaviour and is running at NS 2.3.5 version with predefined devices. As depicted in Table 1, a 400 m ×400 m network size is generated having network size of 200 devices that are mobile in nature and can join and abscond the network at any time randomly. Initially, we have created a network of 5 IoT devices that generates a synthesized information using distribution pattern. Further, to verify the device security, the performance is analyzed in presence of the intruders which has the capability to compromise the legitimate devices in the network. The intruders have used black hole, data falsification, DoS, DDoS and MiTM attacks to disrupt the ideal networking activities.

The malevolent devices are added based on probability during transmission process. Further, Table 2 lists out 200 deployed devices having 50 malevolent nodes. The probability of attacks in a single instance occurs on 3 out of 10, 5 out of 15 and 50 out of 200 devices respectively. The execution is accomplished for 300 seconds.

Table 2: Configuration of Networking Environment

S.No.	Legitimate Nodes	Compromised Nodes
1	10	3
2	15	5
3	200	50

4.2. Performance Parameters

To evaluate the performance of the proposed scheme, we integrated various metrics within the NS-2 simulator including accuracy, response time, resource utilization, authentication delay, end-to-end delay, throughput, probability of attack success and attack detection, to name a few.

Figure 6 provides accuracy to the proposed scheme by detecting the malevolent device in a large number of devices linked to corresponding end users. Accuracy is defined as the difference between actual time and predicted time where the predicted time shows the response time of the devices

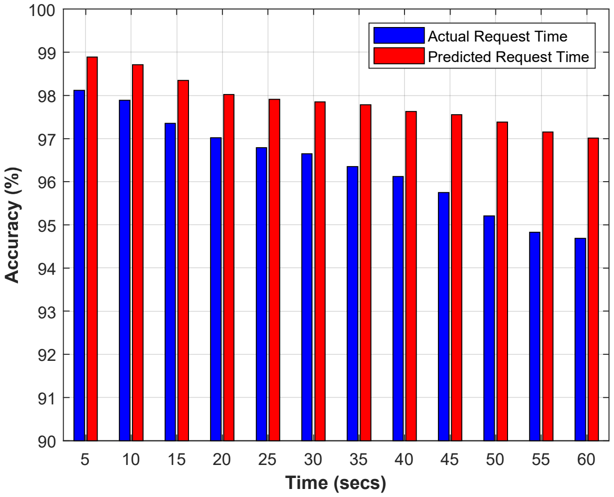

Figure 6: Accuracy Comparison for responding the user's request during malicious devices

under ideal conditions and the actual time show the response time of the devices that are compromised by the intruders. The proposed scheme achieves better accuracy for the malicious device prediction which may be further enhanced if simulation runs for a longer period of time. The main reason behind this high accuracy is the trust model that is computed through PHI enables the legitimate devices to identify malicious nodes and thus revoke them from the network.

Further, it is predicted that the response time from IoT devices for the proposed scheme performs better as depicted in Figure 7.

It can be clearly seen that the malicious devices are identified using trust and are removed from the network that further leads to increase in response time and efficiency of the network. Further, in the proposed scheme the detection of any malevolent device is immediately followed by its removal from the networks so that it does not affect the overall network performance.

Next, we evaluated the proposed mechanism against existing approach over various measuring parameters such as resource utilization and number of processed request. This analysis further shows an improvement in resource utilization as revealed in Figure 8.

The resource utilization parameter depicts the number of network resources to be used by the IoT devices while communicating or providing the requested services of the users. The resource utilization of proposed phe-

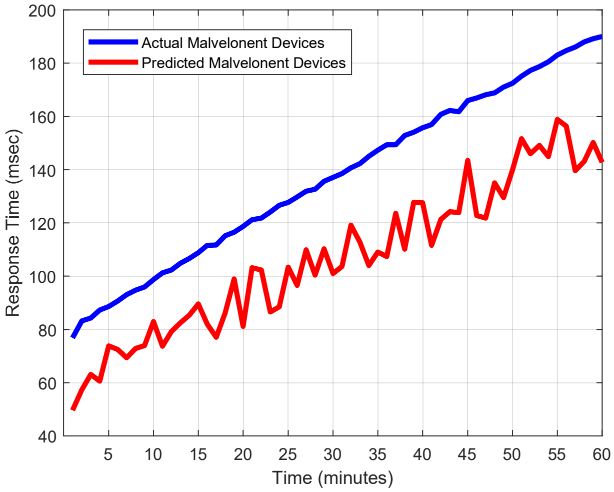

Figure 7: Response Time Comparison for Prediction of Malicious Devices

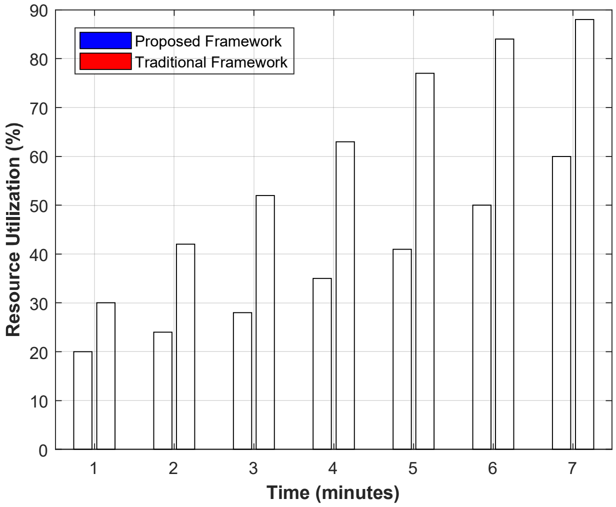

Figure 8: Utilization of resources during malicious environment

nomenon is ideal as compare to existing technique even during the involvement of malicious activities by the intruders. The reason behind this is the involvement of only legitimate devices for providing the data transmission as the malicious nodes are revoked from the network.

Moreover, Figure 9 presents the number of requests processed by the

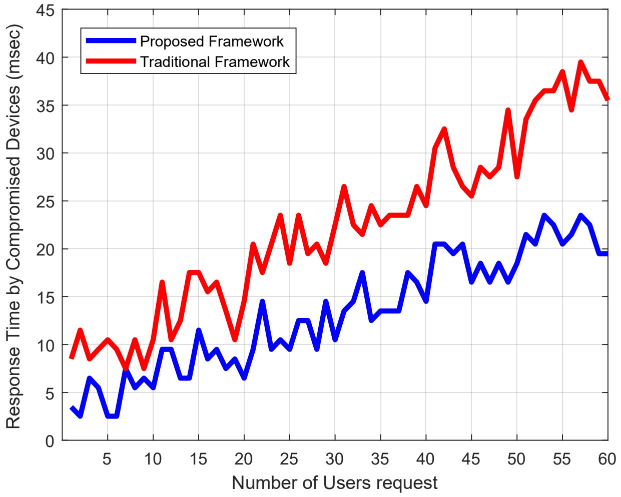

Figure 9: Number of Request Processed with Linear Trend line

proposed system with respect to linear trend for adversary model. It can be seen that as the number of devices increase linearly, the respective number of processed requests also increases linearly. This is due to the fact that our solution relies on trust scheme which eliminates the malicious nodes from the network by identifying their PHI. Hence only legitimate devices are involved during the communication process that can respond to the requested services of corresponding users.

In addition, we analysed our proposed trust-based mechanism for end-to-end delay, network throughput, probability of attack success, ease of attack detection, average and maximum authentication delay. Figure 10 and Figure 11 depicts the end-to-end delay and network throughput for both proposed and existing approaches.

Our proposed solution achieves low end-to-end delay than the existing approach. This is due to the fact that our proposed solution has the ability to detect the malicious and legitimate behaviour of IoT devices at an early stages. Therefore, the overall end-to-end delay decreases as the malicious devices are never involved in the communication process within the network. Similarly, the throughput of proposed approach as depicted in Figure 11 is more than existing mechanism as proposed trust-model never allows malicious number of device to transmit the information in the network.

Further, Figure 12 and Figure 13 measured the probability of attack suc-

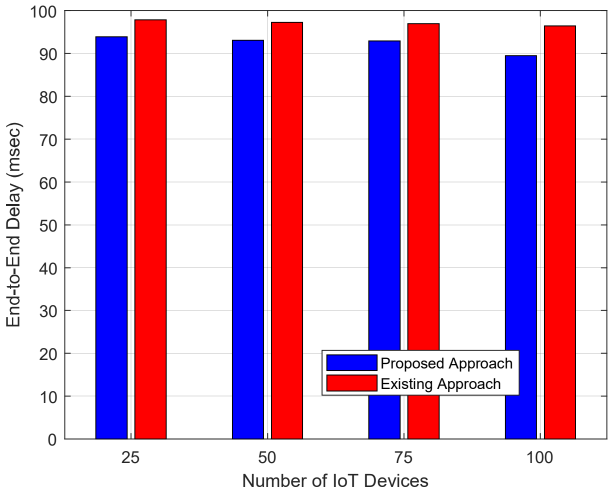

Figure 10: End-to-End delay over Number of devices

cess and ease of attack detection in the presence of malicious nodes during communication process.

It can be seen that the proposed mechanism can efficiently detect the malicious behaviour of the nodes and reduces the overall probability of attack success because of its highly trusted nature towards the communicating nodes. The probability of attack success in Figure 12 over 25 MIoT devices is approximately 3.3% due its initial establishment of the network. During the network establishment, a random trust value is assigned to all the devices that allows the intruders to involve at an early stage.

Further, Figure 13 depicts that the probability of attack detection over 25 MIoT devices is higher which further reduces at a consistent rate. The major reason behind this phenomenon is that as the number of nodes increases, the already existing legitimate devices may get compromised by the intruders. The compromised devices may further generate various attacking patterns and strategies such as sybil attack and worm hole attack which are very difficult to detect at first instance.

These attacking strategies can be further identified through trust computation and their previous behaviours upon increasing the number of nodes with a larger rate. Finally, Figure 14 presents the average and maximum authentication delay of proposed and existing approaches over various number of devices.

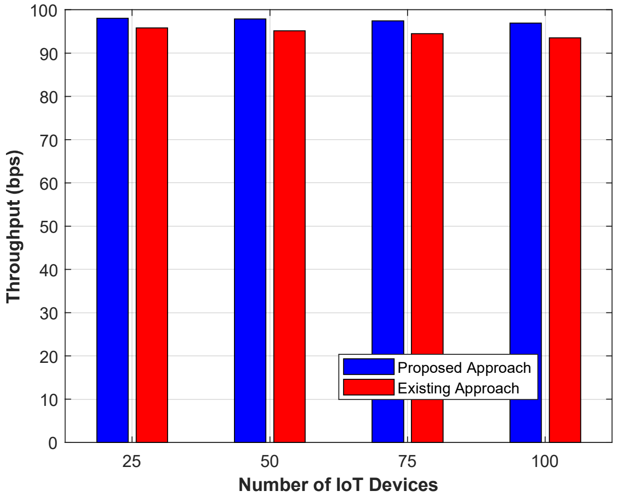

Figure 11: Throughput over Number of devices

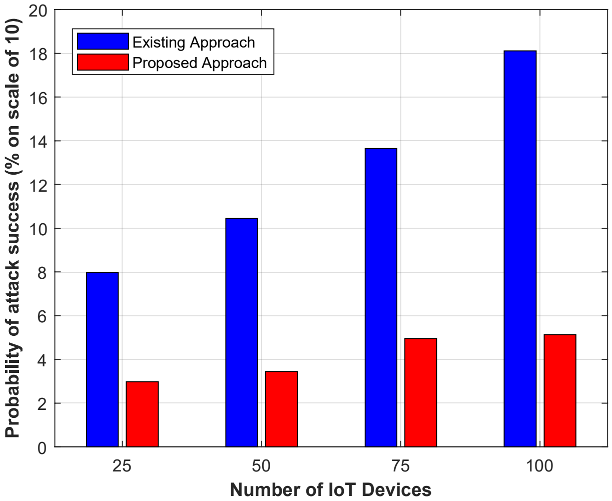

Figure 12: Probability of attack success over Number of devices

Average and maximum authentication delay signifies the amount of time required to authenticate a node before participating into communication process. The authentication of legitimate and malicious devices through trust computation ensures efficient and fast detection process as compared to other existing techniques. In a brief, all the above results depict the superior behaviour of the proposed scheme because a reference from the database of

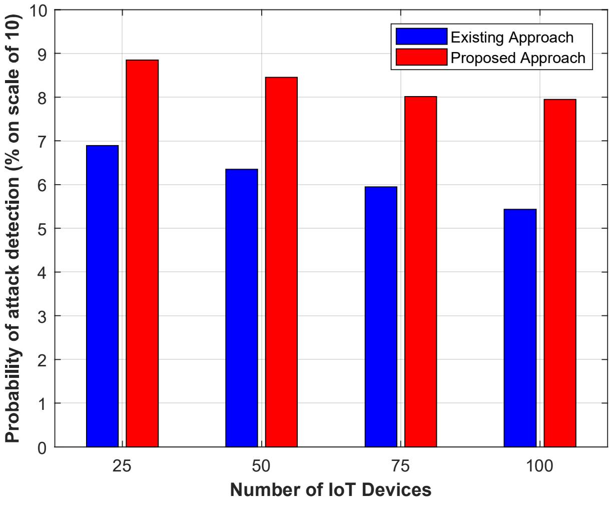

Figure 13: Probability of attack detection over Number of devices

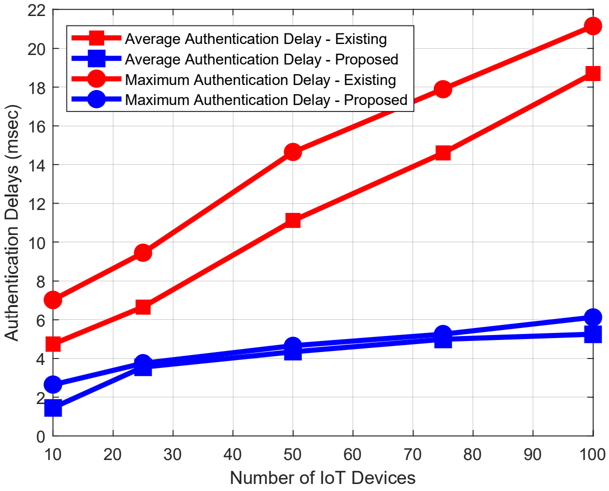

Figure 14: Average and Maximum Authentication Delay over Number of devices

former interactions results in a drop of the malicious nodes forever which enhances the network performance in terms of cost and resource utilization.

Furthermore, Figure 15 and Figure 16 depicts DoS and DDoS attacks that are more specific to MIoT architectures. In the depicted Figure 15, proposed scheme outperforms existing approach as it integrates a trusted routing procedure where malicious devices are identified and eliminated before starting the communication mechanism.

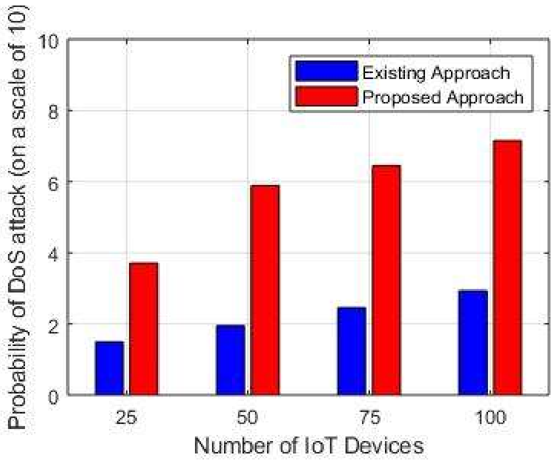

Figure 15: DoS attack over Number of devices

Similarly in Figure 16, our proposed solution is more resilient to DDoS attacks as compared to the existing approach as it can identify attackers at an early stage of the communication process.

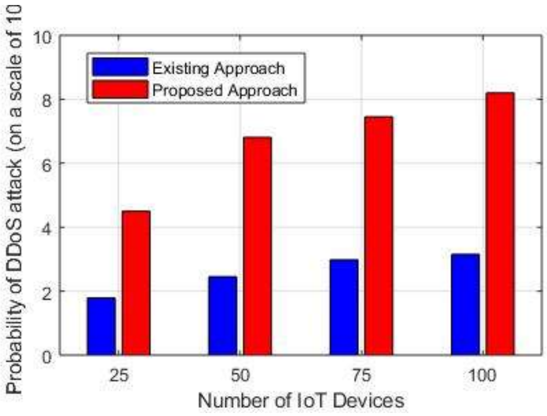

Figure 16: DDoS attack over Number of devices

4.3. Results Discussion

Proposed and existing mechanisms have been appraised based on various network environments and devices for which a personalized simulation has been projected.We conducted a simulation-based study to validate our proposal which is depicted by the simulation results in previous section.

From the results, we can conclude that the accuracy of our proposed trust-based solution was close to 94% which can further be enhanced if the simulation time is high due to the fact that the devices spent higher time in the network which can be further identified via their trust values. Moreover, the response time will be rapid because of identification and removal of detected malevolent devices from the system. The identification and detection of malevolent devices was computed through device trust. Lastly, we concluded that our proposed scheme can efficiently detect and identify malevolent devices as depicted by the simulation results. The main reason of the proposed scheme out performance as compared to existing technique is its reliance on the data of PHI. As the existing technique identifies the nodes' legitimacy based on their current reputation and interaction which can be tampered by the malicious behaviour of the nodes, thus achieving low performance in comparison to the proposed approach. However using the PHI scheme, whenever a node performs malicious activity, its performance based on energy consumption and packet loss ratio is recorded in the database which is used for future inference in calculating the trust. Further, the early stage identification of malicious devices and their blockage for participating in the communication process makes better utilization of resources and highlights it better as compared to existing approach. Further, the use of Johnson's algorithm to route the messages through shortest path reduces the response time among devices and requested user's.

5. Conclusion

In order to solve various contemporary issues of IP networks, NDN have been proposed as a future networking paradigm. Though it provides an additional security layer by knowing the data to only sender and receiver, however, it has numerous setbacks such as complex security cost, computation communication overhead etc. Recently, trust-based mechanisms have been proposed by few researchers in content delivery mechanism in NDN, however, only few of them have used trust scheme for identifying the device's legitimacy. In this paper, we proposed a secure trust-based solution to compute the legitimacy of MIoT devices based on various parameters such as energy consumption while transferring the data, message delivery to preceding or succeeding nodes, distance among two devices to identify denial of service and man-in-middle attack and so on. Simulation results depicted that our proposed trust-based mechanism efficiently verified several parameters such as accuracy, response time, resource utilization and number of proposed requests against traditional mechanism. The simulated results against various parameters show approximate 94% success rate in the proposed framework as compared to traditional approach.

In future, we will report the identification of specific NDN threats with their resolution mechanism by integrating blockchain within MIoT networks. Further, the tradeoff between delay and power during node security will also be taken up for prospective scrutinizing. Moreover, the real-time scenarios communication, congestion overheads while processing the data or services through legitimate trusted node's can be further analyzed.

References

References

[1] I. Farris, L. Militano, M. Nitti, L. Atzori, A. Iera, MIFaaS: A Mobile-IoT-Federation-as-a-Service Model for Dynamic Cooperation of IoT Cloud Providers, Future Generation Computer Systems 70 (2017) 126–137.

[2] C. Marxer, C. Tschudin, Schematized Access Control for Data Cubes and Trees, in: Proceedings of the 4th ACM Conference on Information-Centric Networking, ACM, 2017, pp. 170–175.

[3] E. Baccelli, C. Mehlis, O. Hahm, T. C. Schmidt, M. Wählisch, Information Centric Networking in the IoT: Experiments with NDN in the Wild, in: Proceedings of the 1st ACM Conference on Information-Centric Networking, ACM, 2014, pp. 77–86.

[4] Z. Yan, S. Zeadally, Y.-J. Park, A Novel Vehicular Information Network Architecture based on Named Data Networking (NDN), IEEE internet of things journal 1 (6) (2014) 525–532.

[5] W. Shang, A. Bannis, T. Liang, Z. Wang, Y. Yu, A. Afanasyev, J. Thompson, J. Burke, B. Zhang, L. Zhang, Named Data Networking of Things, in: IEEE first international conference on internet-of-things design and implementation (IoTDI), IEEE, 2016, pp. 117–128.

[6] V. Perez, M. T. Garip, S. Lam, L. Zhang, Security Evaluation of a Control System using Named Data Networking, in: 21st IEEE International Conference on Network Protocols (ICNP), IEEE, 2013, pp. 1–6.

[7] P. Gasti, G. Tsudik, E. Uzun, L. Zhang, DoS and DDoS in Named Data Networking, in: 22nd International Conference on Computer Communication and Networks (ICCCN), IEEE, 2013, pp. 1–7.

[8] C. Ghali, G. Tsudik, E. Uzun, Network-layer Trust in Named-Data Networking, ACM SIGCOMM Computer Communication Review 44 (5) (2014) 12–19.

[9] F. G. Mármol, G. M. Pérez, Security Threats Scenarios in Trust and Reputation Models for Distributed Systems, computers & security 28 (7) (2009) 545–556.

[10] M. Pearce, S. Zeadally, R. Hunt, Virtualization: Issues, Security Threats, and Solutions, ACM Computing Surveys (CSUR) 45 (2) (2013) 17.

[11] Z. Wei, F. R. Yu, A. Boukerche, Trust based Security Enhancements for Vehicular Ad Hoc Networks, in: Proceedings of the fourth ACM international symposium on Development and analysis of intelligent vehicular networks and applications, ACM, 2014, pp. 103–109.

[12] L. Gu, J. Wang, B. Sun, Trust Management Mechanism for Internet of Things, China Communications 11 (2) (2014) 148–156.

[13] M. A. Hail, M. Amadeo, A. Molinaro, S. Fischer, Caching in Named Data Networking for the Wireless Internet of Things, in: IEEE International conference on recent advances in internet of things (RIoT), IEEE, 2015, pp. 1–6.

[14] M. Liu, T. Song, Y. Yang, B. Zhang, A Unified Data Structure of Name Lookup for NDN Data Plane, in: Proceedings of the 4th ACM Conference on Information-Centric Networking, ACM, 2017, pp. 188–189.

[15] S. Tiennoy, C. Saivichit, Using a Distributed Roadside Unit for the Data Dissemination Protocol in VANET with the Named Data Architecture, IEEE Access 6 (2018) 32612–32623.

[16] B. Nour, K. Sharif, F. Li, Y. Wang, Security and Privacy Challenges in Information-Centric Wireless Internet of Things Networks, https://hal.archives-ouvertes.fr/hal-02189504 (Jul. 2019).

[17] B. Nour, K. Sharif, F. Li, S. Yang, H. Moungla, Y. Wang, ICN Publisher-Subscriber Models: Challenges and Group-based Communication, IEEE Networkdoi:10.1109/MNET.2019.1800551.

[18] Z. Zhang, Y. Yu, H. Zhang, E. Newberry, S. Mastorakis, Y. Li, A. Afanasyev, L. Zhang, An Overview of Security Support in Named Data Networking, IEEE Communications Magazine 56 (11) (2018) 62–68.

[19] Y. Yu, Y. Li, X. Du, R. Chen, B. Yang, Content Protection in Named Data Networking: Challenges and Potential Solutions, IEEE Communications Magazine 56 (11) (2018) 82–87.

[20] D. Rezende, C. Maziero, E. Mannes, A Distributed Online Certificate Status Protocol for Named Data Networks, in: Proceedings of the 33rd Annual ACM Symposium on Applied Computing, ACM, 2018, pp. 2102–2108.

[21] Z. Zhang, A. Afanasyev, L. Zhang, NDNCERT: Universal Usable Trust Management for NDN, in: Proceedings of the 4th ACM Conference on Information-Centric Networking, ACM, 2017, pp. 178–179.

[22] C. Tschudin, E. Uzun, C. A. Wood, Trust in Information-centric Networking: From Theory to Practice, in: 2016 25th International Conference on Computer Communication and Networks (ICCCN), IEEE, 2016, pp. 1–9.

[23] Y. Yu, A. Afanasyev, D. Clark, V. Jacobson, L. Zhang, et al., Schematizing Trust in Named Data Networking, in: Proceedings of the 2nd ACM Conference on Information-Centric Networking, ACM, 2015, pp. 177–186.

[24] B. Nour, K. Sharif, F. Li, S. Biswas, H. Moungla, M. Guizani, Y. Wang, A Survey of Internet of Things Communication using ICN: A Use Case Perspective, Computer Communicationsdoi:10.1016/j.comcom.2019.05.010.

[25] A. Aboodi, T. Wan, G. Sodhy, Survey on the Incorporation of NDN/CCN in IoT, IEEE Access 7 (2019) 71827–71858. doi:10.1109/ACCESS.2019.2919534.

[26] T. Mick, R. Tourani, S. Misra, LASER: Lightweight Authentication and Secured Routing for NDN- IoT in Smart Cities, IEEE Internet of Things Journal 5 (2) (2017) 755–764.

[27] K. Lei, S. Zhong, F. Zhu, K. Xu, H. Zhang, An NDN IoT Content Distribution Model with Network Coding Enhanced Forwarding Strategy for 5G, IEEE Transactions on Industrial Informatics 14 (6) (2017) 2725–2735.

[28] K. Zhu, Z. Chen, W. Yan, L. Zhang, Security Attacks in Named Data Networking of Things and a Blockchain Solution, IEEE Internet of Things Journal 6 (3) (2019) 4733–4741. doi:10.1109/JIOT.2018.2877647.

[29] W. Fang, M. Xu, C. Zhu, W. Han, W. Zhang, J. J. Rodrigues, FETMS: Fast and Efficient Trust Management Scheme for Information-Centric Networking in Internet of Things, IEEE Access 7 (2019) 13476–13485.

[30] S. Signorello, M. R. Palattella, L. A. Grieco, Security Challenges in Future NDN-enabled VANETs, in: IEEE Trustcom/BigDataSE/ISPA, IEEE, 2016, pp. 1771–1775.

[31] D. B. Johnson, Efficient Algorithms for Shortest Paths in Sparse Networks, Journal of the ACM (JACM) 24 (1) (1977) 1–13.