ISSN: 2834-7706

Research Article

Journal of Mathematical Techniques and Computational Mathematics

Secure PRoPHET-Based Routing Protocol for Mobile IoT Networks using RAID5 Technique

Ridouane El Mezouary*

ENSIAS, Mohammed V University of Rabat, Morocco

***Corresponding Author**
Ridouane El Mezouary, ENSIAS, Mohammed V University of Rabat, Morocco.

Submitted: 2024, Sep 02; **Accepted:** 2024, Sep 30; **Published:** 2024, Oct 23

Citation: Mezouary, R. E. (2024). Secure PRoPHET- Based Routing Protocol for Mobile IoT Networks using RAID5 Technique. *J Math Techniques Comput Math, 3*(10), 01-07.

Abstract

The important moving towards the Internet of Things (IoT) induced a huge increase in the number of connected physical devices. Mobile computing is emerging to manage the vast amount of data produced. Moreover, it meets the demand for more complex IoT applications. Therefore, the probabilistic routing in mobile IoT networks is developing very fast and offering new perspectives. This type of routing uses the mobility history when making a forwarding decision. However, despite this development, There is the network security problem. The latter becomes indispensable and requires that the mobile IoT networks to be well protected against different attacks. In this article, we propose a new secure probabilistic routing protocol PRoPHET-RAIP5, which is the secure version of the probabilistic protocol PRoPHET. To do so, we used the RAID5 technology and a multi-path routing. We have implemented our solution on the PRoPHET protocol. Finally, We compared our PRoPHET-RAIP5 protocol with the standard PRoPHET protocol, to evaluate the performance of both protocols in terms of security.

Keywords: Internet of Things (IoT), Security, Probabilistic Routing, PRoPHET, Multipath Routing, PRoPHET-RAIP5, Attack, RAID5

1. Introduction

The Internet of Things (IoT) is no longer a fantasy of science fiction. Advances in technology allow now the con- nection of everyday objects to the Internet. Open and inter- operable solutions must however be used to ensure an optimum communication between these objects. In this context, the routing protocol is a the key element which allows for each object to communicate with other objects. Sensors have long been simply used to quantify and monitor a physical value locally: sensor of a gas in a plant, temperature in the home, brightness for urban lighting. The advent of the Internet and research in the field of wireless technologies have provided these sensors with connectivity and given rise to wireless sensor networks. The generalization of these sensors has led to the creation of a multitude of new applications: monitoring the energy consumption of a home, management of urban traffic lights or intelligent lighting system for a municipality. In a broader sense, wireless sensor networks can be seen as a subset of the broader concept of the Internet of Things. The Internet of Things aims to provide connectivity to a heterogeneous set of everyday objects using wired or wireless communications. Nowdays, IoT networks must be secure. It must offer a good level of quality of service for users.

The authors of use the potential of mobile computing to improve the analysis of IoT application data. This is while ensuring data security and computational efficiency [1]. More specifically, they examined MEC (Mobile edge computing) and several MEC-assisted IoT applications. An Experience- Reputation was proposed in the, which presents a new confidence assessment mechanism.It uses trust relationships between mobile devices on a platform called MCS (Mobile Crowd-Sensing) [2]. It includes trustworthy indicators called repu- tation. In the research study, the authors use the blockchain which is a disruptive technology, and which has gained wide recognition among the experts of various domains [3]. In the same work, the authors examine the applications of the backchain and its interaction with the Internet of Things. Authors of show how nanoelectronic PUF (physically unclonable function) can used in security applications, example of authentication[4]. In the work, the authors offer a detailed analysis of trust management techniques and security issues adapted by IoT, to secure data in a cloud environment [5]. In article, the authors describe a solution of monitoring that is based on slight behavior [6]. This is aiming to determine the incorrect behavior of an integrated IoT device. The authors have shown that the technique of incorrect behavior detection, based on the specification of rules, exceeds the techniques of anomalous behavior detection based on the anomalies for an UAV (unmanned aerial vehicle) cyber-physical system. The

authors in introduces a configurable security framework based on edge computing, which uses a peripheral periphery close to the user, with a large computing capacity to secure an IoT network. Moreover, based on this framework, it is possible to design a configurable security function protocol, interacting with an SA (security agent), to meet the requirements of security [7]. In, the authors show some basic models in IoT system. They have cracked cryptographic methods to preserve the confidentiality of the data in these models [8]. In the study paper, the authors use the attack models for IoT applications. They also offer machine learning as a security solution [9]. The authors in use an IoT infrastructure. Data is stored in this infrastructure using an attack-resistant and fault-tolerant system [10].

In this paper, we exploit the mobility of connected physical devices and the predictability of meeting, to ensure data confidentiality, data integrity, and network availability, while improving packet delivery ratio (PDR) in mobile IoT networks. More precisely, we propose a new secure routing protocol for IoT network. This protocol makes it possible to divide the message into two parts, then calculate their XOR to build part 3, at the source level. Then transmit these three parts in three disjoint paths, to reach the destination, to build the initial message again. Part 3 checks the integrity of the message at the destination level, by comparing the XOR of part 1 and part 2 at the destination level with part 3, which contains the XOR of part 1 and part 2 calculated at the source level. If they are equal, then the message is not modified, if not then the message is modified.

This article is organized as follows: Security in mobile IoT networks is presented in section II. The RAID5 technique is introduced in the section III. Section IV details our PROPHET-RAIP5 protocol. Section V presents simulation results. Finally, Section VI summarizes the article and presents some perspectives.

2. Security in mobile IoT networks

To ensure the security of routing in a mobile IoT network, the objects must execute the security mechanismsthemselves. This aims to protect it against attacks due to lack of centralized infrastructure which could manage the security service. In a mobile IoT network, objects don't have strong computing, storage, and energy capabilities. Indeed, the use of security systems based on key encryption consumes more resources. This can significantly affect the performance of the routing in the network. Research works proposed for mobile IoT networks attempt to establish a compromise between the ro- bustness of the proposed security solution and its effectiveness.

2.1 Security Principles For Mobile IoT Networks

Computer security is a set of techniques that ensure the proper functioning of the hardware or software resources of an information system. Mobile IoT networks require solutions that ensure the security of messages sent over the network. This is in different military applications, environmental, med- ical, and surveillance. The security of messages in mobile IoT networks must meet the following key security objectives:

2.1.1 Confidentiality of the Data

The network must ensure that the data circulating through the network is confidential. Confidentiality prevents data to be consulted by unauthorized devices or persons. In a mobile IoT network, strict access controls must be in place to ensure data privacy. Confidentiality is important in medical applications, where this kind of information has not to be disclosed. Moreover, it is relevant also in military applications, where information can have strategic consequences on real actions on the ground.

2.1.2 Data Integrity

This service ensures that data should not be corrupted during the communication. The destination verify that the message received is the same as the message sent. Data integrity is an important requirement for mobile IoT networks. It must therefore be ensured that no one can modify the data. It can be questioned by many events. Among these, attacks aimed at modifying the content of the messages and the low reliability of the wireless links.

2.1.3 Network Availability

The network must be available at any time and the sending of information should not be interrupted. For a mobile IoT network, each connected device that detects an event can transmit it at any time to the gateway.

The RPoPHET-RAIP5 protocol permits to ensure these three security objectives. This is by using the principle of the segmentation of the message in source object. Then to send the three parts of the message in disjoint paths. And finally the construction of the message in the destination (gateway), which will be detailed in the description part of the probabilistic protocol PRoPHET-RAIP5. It will be checked in the simulation part of the PRoPHET-RAIP5 protocol.

2.2 Attacks Against Mobile Iot Networks

In a mobile IoT network, each object can intervene in the communication. There may be malicious objects in the network, which aim to disrupt the traffic flowing in the network, or disturb the routing process. This aims to find the compromise between confidentiality and data integrity in the network. In a mobile IoT network, there are several attacks that can affect its proper functioning. Some aim to reduce the availability of the network, others aim to affect the integrity of the messages circulating in the network. We present below two types of attacks in mobile IoT networks:

2.2.1 Black-Hole Attack

In this attack, the malicious object creates a kind of sink or "black hole" in the network. It appears to the other objects as being an attractive object. It looks for possible paths that control most of the data passing through the network. This is by placing itself at a strategic place in the network to force the passage of data through itself. Then it deletes all received messages. This kind of attacks will be studied in this article, and observe the reaction of the probabilistic protocol PRoPHET-RAIP5 against it.

2.2.2 Modification Attack

A malicious object will retrieve a message and modify it. This is by adding false infor- mation to it, or destroying packets to make the message incomprehensible. This attack will be treated also in this article, and we present the behavior of the probabilistic

protocol PRoPHET-RAIP5 against this attack, and the role that probabilistic protocol PRoPHET-RAIP5 will play in this case.

In this article, we propose to secure the routing process for mobile IoT networks against of attacks (insertion attack, black hole attack). This by using the data backup technology RAID5 (Redundant Array of Independent Disks 5) and the probabilistic routing protocol PRoPHET.

3. Raid5 Technique

In an information system, data is the most sensitive resource. Indeed, we need a protection method that ensures that the data is protected, and accessible without interruption. This is in case of failure of the hard drive in which the data is stored. One of the most common used method is the RAID (Redundant Arrays of Inexpensive Disks) technique. The latter is a collection of techniques which distribute data across multiple disks. This aims to improve data security, fault tolerance or system performance. There are several levels of the RAID system; each level defines a degree of reliability and performance. We present below the RAID5 level, which will be exploited in this article, to secure the routing of information in a mobile IoT network.

The RAID5 is known by the name "volume aggregated by distributed parity bands", this level allows to combine the two levels RAID0 (ensure data continuity) and RAID1 (ensure data availability). It must contain at least three disks and we separate the parity disk on several disks (Figure 1). This solves the problem of parity disk throttling. RAID5 has become the benchmark of server environments requiring fault tolerance capability. In case of a physical disk failure, it recreates its contained data from the parity and the remaining data. This level presents a good solution to ensure data redundancy in a computer environment.

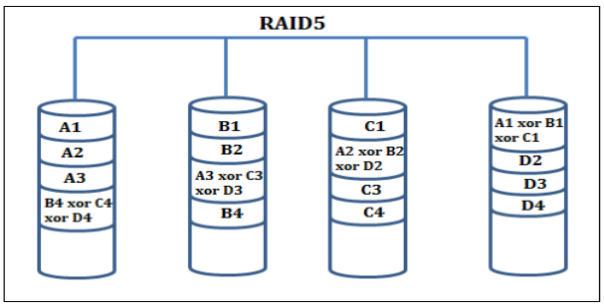

Figure 1: RAID5 Operating Diagram

4. Probabilistic Protocol PRoPHET-RAIP5: Description and Presentation

In an IoT network, sending the entire message in one path between the source (connected device) and destination (gateway) increases the complete message loss risk (black hole attack), or may be modified which induced the message wrong reception (insertion attack). This makes the possibility that these attacks exist in the network by a malicious connected device (passive listening attack).

Probabilistic routing uses the story of meeting nodes to make a decision to send a message. Indeed, we thought to make this type of routing more reliable and well secured. Aiming to provide users with a high quality of service for all applications in IoT. It is in this context that we proposed PRoPHET-RAIP5, which is a secure routing protocol proposed for mobile IoT networks. It is based on the RAID5 technique, multi-path routing, and PRoPHET Protocol. The principle of this protocol is instead of sending the packet by a single path chosen by the protocol; the source will share it on three disjoint paths. Then, we used the RAID5 technique to ensure availability, the confidentiality and integrity of the data received.

The principle of this approach is that the source connected device:
i) divides the message to send in two parts P_1 and P_2,
ii) calculates their XOR to build the P_3 part,
iii) encapsulates each part in a packet, then
iv) transmits these three packets in three disjoint paths to reach the destination (gateway).
This will help to reconstruct the initial message. We describe below the operating principle and the different operations of the PRoPHET-RAIP5 protocol:

4.1 Step 1: Division of the Message in the Connected Device

The first stage of this action is to generate the message that will be processed and transmitted. This message is generated at the application layer. Moreover, we have considered the CBR traffic (Figure 2) that is characterized by a constant flow. Besides, this traffic will then be attaching by the UDP transport agent that will carry the packets to the destination (gateway). Then, the connected device will divide the message into two parts P_1 and P_2. However, to build the part P_3, it calculates the XOR (exclusive or) of both parts P_1 and P_2.

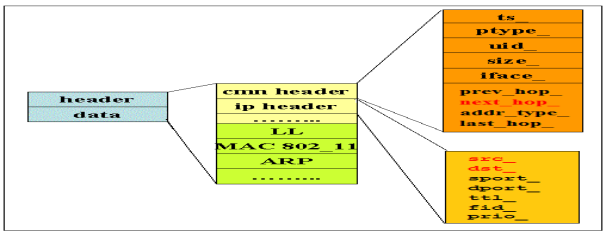

Figure 2: Structure of a CBR Packet

The generated CBR traffic uses the connections that carry traffic at a constant bit rate, and intended for real-time appli- cations. Figure 3 shows an example of the traffic generation code, that creates a connection between the source (connected device) and the destination (gateway). Among the character- istics of this traffic, we find:

4.1.1 The packet size is 512 bytes.

4.1.2 The maximum number of packets sent is 1000 packets.

```
set cbr_(0) [new Application/Traffic/CBR]
$cbr_(0) set packetSize_ 512
$cbr_(0) set interval_ 3
$cbr_(0) set random_ 1
$cbr_(0) set maxpkts_ 1000
$cbr_(0) attach-agent $bundle_(1)
$bundle_(1) conect $bundle_(2)
$ns_ at 25.561746128630705 "$cbr_(0) start"
```

Figure 3: CBR Traffic Generation Code

With probabilistic protocol PRoPHET-RAIP5, UDP trans- port agent will be able to insert the three packets instead of a single packet. The first packet will encapsulate the first half of the message, the second takes care of the second half of the message, and the third will take the message that contains the XOR of the two halves of the message. If the message size is odd, character 0 will be added to the end of the string (which presents the message). After having each part of the message encapsulated in a packet, and that the destination (gateway) may order the parts to receive the message, the first part will be identified by the number 1, the second part by the number 2 and the third part by the number 3 (Figure 4).

4.2 Step 2: Sends Packets in Disjoint Paths

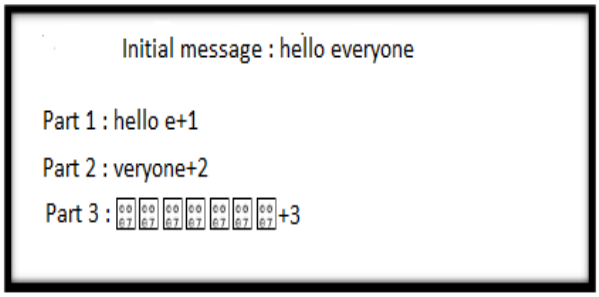

Figure 4: Example of Dividing the Message

After generating the message in the application layer of the connected device, The source node cuts the message in two parts, calculates their XOR, and attaches the parts by a transport agent. Then it will route the packets in the network layer to the destination (gateway) in three disjoint paths. The probabilistic protocol PRoPHET-RAIP5 sends the three parts of the initial message in three disjoint paths of the mobile IoT network. It aims to avoid the risk that the three parts of the message or at least two parts of the message will pass on the same malicious connected device. It may cause an entire loss of message in the first scenario. Moreover, in the second scenario, we cannot build the initial message with only one part of the message. This is especially when the network is attacked by a black hole attack or a modification attack or other attacks.

The probabilistic protocol PRoPHET-RAIP5 works in mo- bile environment. However, to transmit the three parts of the departure message on paths disjoints, we assume that each connected device (relay) can receive one of the three parts as maximum of the message generated by the connected device source. This excepts the destination (gateway) that can receive and process the three parts of the message.

Figure 5 presents an example of sending three parts of the initial message from the connected device (source) to the desti- nation (gateway) in three disjoint paths. The source connected device meets first the connected device 7, it sends to it the first part that will transmit it directly to the destination (gateway). The second part will be transmitted to the connected device. Then, it will in turn meet the connected device 9 which will transmit the second part to the destination (gateway). The third part will be transmitted to the connected device 8. Then to the connected device 4 which will transmit to the destination (gateway). The connected device 9 can't receive part 1 of the message from connected device 7. This is because it already received the second part of the same message.

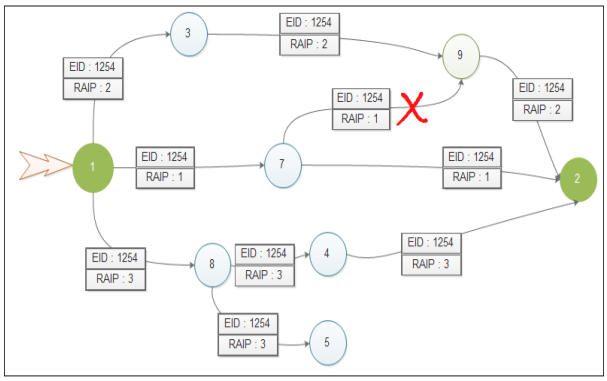

Figure 5: Example of Sending Parts of the Message in Three Disjoint Paths

4.3 Step 3: Reconstruction of the Message in the Destination

After sending the three parts of the message in disjoint paths, the destination must order them according to the identi- fication codes. This is to differentiate between the parts of the message (when the gateway (destination) receives the packets). This aims to reconstruct the original message and verify its integrity. At this level, three scenarios are possible:

• The gateway (destination) receives a packet among the three sending packets. In this case the gateway (destination) will not be able to reconstruct the initial message.

• The gateway (destination) receives two parts out of three, which induces that two cases are possible: if it receives P_1 and P_2, it can reconstruct the initial message directly. If it receives (P_1 or P_2) and P_3, it recovers (P_2 or P_1) by calculating the XOR between (P_1 or P_2) and P_3. Then it reconstructs the initial message from P_1 and P_2.

• The gateway (destination) receives the three packets without loss, in this case we will concatenate the first with the second half to reconstruct the initial message. Afterwards, to check the integrity of the message, the gateway (destination) recalculates the XOR of the first two halves, and compares it with the third received packet that contains the XOR calculated by the connected device source.

5. Simulation Results

In an IoT network, we often consider objects (sensors) that have hardware and software constraints that do not allow them to connect directly to the Internet. They connect through a gateway. Indeed, the Internet is not dimensioned to manage the addressing of connected objects. In this paper, we con- sider RRoPHET and PRoPHET-RAIP5 probabilistic routing protocols. We compared their performance in terms of security, to ensure communication between connected physical devices (usually sensors) and gateways (destinations).

Gateways act as intermediaries to connect the object to the internet and send its data to the cloud. An example of these gateways are home routers (case of an intelligent home) and mobile phones too. These gateways provide what is needed in terms of connectivity, security and device management. Gateways also translate proprietary protocols (PRoPHET and PRoPHET-RAIP5 in our case) to the Internet and some may act

as network aggregators.

We are starting the experimental study on the probabilistic protocol PROPHET-RAIP5. In this section, we study the protocol behavior of the probabilistic protocol PRoPHET- RAIP5 in an attack environment. We simulate in the first part the probabilistic protocol PRoPHET-RAIP5 with the modifi- cation attack. In the second part we simulate the probabilistic protocol PROPHET-RAIP5 with the black hole attack. In both cases we compare the results obtained from the probabilistic protocol PRoPHET-RAIP5 with the standard PRoPHET pro- tocol.

5.1 PRoPHET-RAIP5 Protocol and Modification Attack

We did this part of simulation using the NS2 simulator. In this first attack, the attacker represented by a malicious connected device modifies transmitted information. It may also inject other erroneous messages. This has a dangerous impact when the information is sensitive and important, such as the case of exchange of public or even private keys. Therefore, if the destination gateway accepts any message received without integrity check, it may accept erroneous messages.

To illustrate the behavior of the probabilistic protocol PRoPHET-RAIP5 aimed at the modification attack, we considered a mobile IoT network shown in Figure 6. The connected device source of the initial message which is ”hello everyone” is the connected device ”1”. Then, the gateway is the device ”2”, which plays the role of the destination of the message. Moreover, the connected device ”8” will play the role of the attacker that will alter the message. Figure 7 gives an overview of the trace file, which contains all the events of the modified attack simulation.

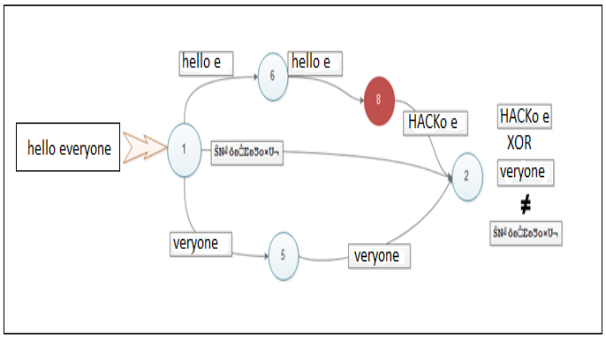

Figure 6: Modification Attack Simulation Scenario

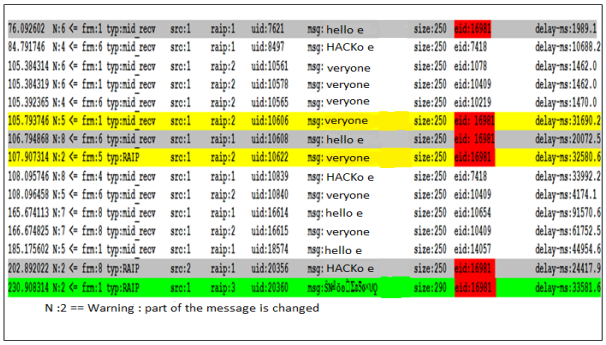

Figure 7: Result of Modification Attack

The starting message is ”hello everyone”, which will be peeled in two parts ”hello e” and ”veryone”. The connected device source will then calculate their XOR to build the third part. Then, the three parts will be sent in three ways disjointed as shown in Figure 6. In this considered scenario, the first part of the message ”hello e” took the path $1 - 6 - 8 - 2$ (Figure 6). The trace of the packet is highlighted in gray (Figure 7). Moreover, at the moment 76.0926 seconds the packet arrives at the connected device ”6” from the source (connected device ”1”), having 250 bytes as size, with a delay of 1989.1 milliseconds. At the instant 106.7948 seconds, the connected device ”6” sends the packet to the connected device ”8”, which will modify its contents by replacing the first four characters ”hell” by the string ”HACK”. Eventually, the altered message will reach the destination gateway at the instant 202.89 seconds.

The second part of the message ”veryone” took the path $1 - 5 - 2$ (Figure 6). The trace of the packet is highlighted in yellow (Figure 7). It shows the transition of the packet from the connected device source passing at the moment 105,7937 seconds by the connected device ”5”. Then, the connected device ”5” transmitted the packet to the destination gateway at the instant 107,9073 seconds.

The third part, which contains the XOR of the two halves of the message, was received directly from the connected device source to the destination gateway (Figure 6), at the moment 230,9083 seconds. Its trace is highlighted in green (Figure 7). It contains a message that is not readable, because the contents of its characters do not correspond to that of the alphanumeric characters.

The following case is for an attack generated by the con- nected device ”8”, which changes the characters ”hell” by a ”HACK” during its transmission. In the case of the standard PRoPHET protocol, the destination gateway will accept the erroneous message as it is, because it has no way to check the integrity of the message. On the other hand, thanks to our probabilistic protocol PRoPHET-RAIP5 based on the principle of RAID5, the destination gateway will have the opportunity to verify the integrity of the message before accepting it. This is done by means of a comparison between the XOR of the two halves of the message sent and the third packet which contains the XOR calculated by the connected device source. Therefore, if the destination gateway finds these two values equal, the message is then received without any change during the transmission. Otherwise, if it is the case of this attack, the destination gateway will detect that there is a change somewhere, so it will ignore the three packets that build the start message, and report that change to the connected device source to return the message.

5.2 PRoPHET-RAIP5 Protocol and Black Hole Attack

In this second attack [11], the attacker aims to prevent his victim from receiving the messages. The malicious connected device creates a kind of ”black hole” in the mobile IoT network, in our case, the network is mobile. We evaluated the two protocols PRoPHET-RAIP5 and PRoPHET-standard for a mobile IoT network, according to packet delivery ratio, energy consumed, and end-to-end delay. We performed the simulations using NS-2.34. table 1 gives all the simulation parameters.

5.2.1 Packet Delivery Ratio

Parameter	Value
Routing Protocol	Mobile IoT network
Routing Protocol	PRoPHET-RAIP5 PRoPHET-standard
Simulation Time	500 s
Number of nodes	50
Environment Size	$500m \times 500m$
Traffic Type	CBR
Maximum Speeds	10 m/s
Mobility Model	Gauss-Markov

Table 1: Simulation Parameters

Figure 8 represents a comparison between the two proba- bilistic protocols PRoPHET-RAIP5 and PRoPHET-standard, in terms of packet delivery ratio (PDR), as a function of the num- ber of sent packets. When a black hole type attack is generated in the IoT network. In our case, we configured some network objects as black hole attacks. We notice that the PRoPHET- RAIP5 protocol allows an interesting packet delivery ratio (PDR) compared to the PRoPHET-standard protocol. This result is justified by the operation of the PRoPHET-RAIP5 protocol, which makes it possible to build the initial message, at the destination level, using only two parts of the initial message. With the PROPHET-RAIP5 protocol, we generally lose only one part of the three parts of the initial message, attacked by the black hole attack. On the other hand, with the PRoPHET-standard protocol, we lose entire messages attacked by black hole attacks, since it does not have the segmentation with the PRoPHET-standard protocol.

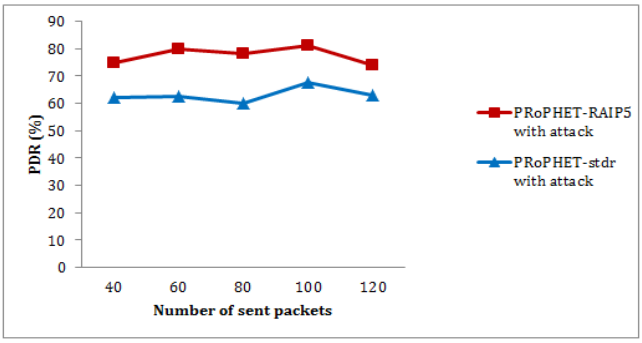

Figure 8: Packet Delivery Ratio vs. Number of Sent Packets

5.2.2 End to End Delay

Figure 9 compares the two protocols PRoPHET-standard and PRoPHET-RAIP5 , according to the end-to-end trans- mission delay, with respect to the sent packets. We notice that the PRoPHET-standard protocol quickly transmitted the messages between the source and the destination, compared to the PRoPHET-RAIP5 protocol. This is explained by the fact that the PRoPHET-RAIP5 protocol processes more packets, because of its packet segmentation system at the source level, the reconstruction of the initial message at the destination level, and sends it from the three parts of the message successively in disjoint paths, all this requires a little more time.

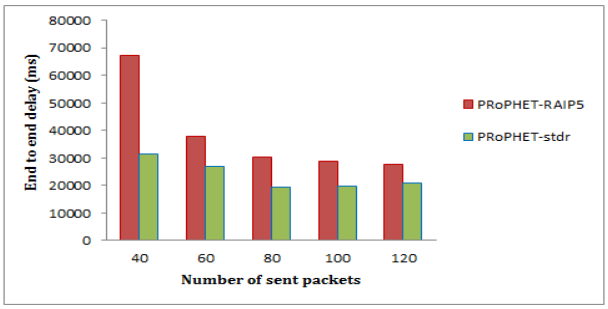

Figure 9: End-To-End Transmission Delay as a Function of Number of Sent Packets

5.2.3 Energy Consumption

Figure 10 gives a comparison between the two probabilistic protocols PRoPHET-RAIP5 and PROPHET-standard in terms of energy consumption. We notice that the standard PRoPHET protocol consumes a little less energy, compared to the PRoPHET-RAIP5 protocol. This result is justified by the fact that the PRoPHET-standard protocol processes and transmits fewer packets. With the probabilistic protocol PRoPHET-RAIP5, we send and receive more packets, because of message segmentation. Indeed as a recapitulation, the more the protocol is secure, the more it consumes energy.

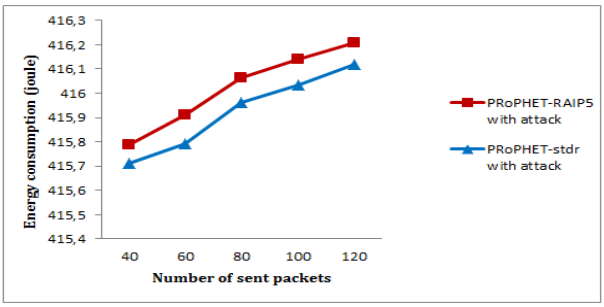

Figure 10: Energy Consumption as a Function of Number of Sent Packets

6. Conclusion

In this article, we presented the secure version of the probabilistic protocol PRoPHET (PROPHET-RAIP5 protocol). We have studied the data processing assisted by mobile connected physical devices for the Internet of Things (IoT) from a security point of view. More precisely, we have used the RAID5 technology, and multi-path routing, to develop a new secure probabilistic routing protocol. This work aims to improve routing performance and secure traffic data in mobile IoT network. However, our choice of the routing protocol focused on the probabilistic protocol PRoPHET. We developed and implemented our solution in this protocol, giving birth to a new probabilistic prtotocol, named PRoPHET-RAIP5, intended for a mobile IoT network. It is to note that the simulations concerned measuring packet delivery ratio for probabilistic protocols standard PRoPHET and PRoPHET- RAIP5, In IoT network with attack. The simulations show that the PRoPHET-RAIP5 protocol provides a good level of security. But it takes a little more time to transmit the data to the destination. It also consumes a little more energy, compared to the standard PRoPHET protocol. At the same time the

probabilistic protocol PRoPHET-RAIP5 ensures data integrity at the destination. What we can't check with the standard PRoPHET protocol.

Finally, as future work, we propose to adapt and implement the method of clustering k-means for the probabilistic protocol PRoPHET-RAIP5, aiming to minimize energy consumption in the network, especially for a mobile IoT network with a high density.

References

1. Ni, J., Lin, X., & Shen, X. S. (2019). Toward edge-assisted Internet of Things: From security and efficiency perspectives. *IEEE Network, 33*(2), 50-57.
2. Truong, N. B., Lee, G. M., Um, T. W., & Mackay, M. (2019). Trust evaluation mechanism for user recruitment in mobile crowd-sensing in the Internet of Things. *IEEE Transactions on Information Forensics and Security, 14*(10), 2705-2719.
3. Kolokotronis, N., Limniotis, K., Shiaeles, S., & Griffiths, R. (2019). Secured by blockchain: Safeguarding internet of things devices. *IEEE Consumer Electronics Magazine, 8*(3), 28-34.
4. Thirukkumaran, R. (2018, November). Survey: security and trust management in internet of things. In *2018 IEEE global conference on wireless computing and networking (GCWCN)* (pp. 131-134). IEEE.
5. You, I., Yim, K., Sharma, V., Choudhary, G., Chen, R., & Cho, J. H. (2018, December). On IoT misbehavior detection in cyber physical systems. In *2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC)* (pp. 189-190). IEEE.
6. Hsu, R. H., Lee, J., Quek, T. Q., & Chen, J. C. (2018). Reconfigurable security: Edge-computing-based framework for IoT. *IEEE Network, 32*(5), 92-99.
7. Wang, W., Xu, P., & Yang, L. T. (2018). Secure data collection, storage and access in cloud-assisted IoT. *IEEE cloud computing, 5*(4), 77-88.
8. Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?. *IEEE Signal Processing Magazine, 35*(5), 41-49.
9. Ozyilmaz, K. R., & Yurdakul, A. (2019). Designing a Blockchain-based IoT with Ethereum, swarm, and LoRa: the software solution to create high availability with minimal security risks. *IEEE Consumer Electronics Magazine, 8*(2), 28-34.
10. El Mezouary, R., Houmz, A., Jalil, J., & El Koutbi, M. (2015, October). PRoPHET-RAIP5: a new approach to secure routing in wireless sensor networks. In *2015 International Conference on Wireless Networks and Mobile Communications (WINCOM)* (pp. 1-6). IEEE.