Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 1468976, 9 pages
https://doi.org/10.1155/2020/1468976

Research Article

Optimized Scheme to Secure IoT Systems Based on Sharing Secret in Multipath Protocol

Fatna El Mahdi,[1] **Ahmed Habbani**,[1] **Zaid Kartit**,[2] **and Bachir Bouamoud**[1]

[1]*SSL Lab, ENSIAS, University of Mohammed V, Rabat, Morocco*
[2]*SIP Research, EMI, University of Mohammed V, Rabat, Morocco*

Correspondence should be addressed to Fatna El Mahdi; fatna.mahdi@um5s.net.ma

Received 29 November 2019; Revised 6 January 2020; Accepted 20 January 2020; Published 4 April 2020

Guest Editor: Hasan Ali Khattak

Internet of Things (IoT) is a hot and emerging topic nowadays. In the world of today, all kinds of devices are supposed to be connected and all types of information are exchanged. This makes human daily life easier and much more intelligent than before. However, this life mode is vulnerable to several security threats. In fact, the mobile networks, by nature, are more exposed to malicious attacks that may read confidential information and modify or even drop important data. This risk should be taken in consideration prior to any construction of mobile networks especially in the coming 5G technology. The present paper aims to provide a contribution in securing such kinds of environment by proposing a new protocol that can be implemented in ad hoc networks.

1. Introduction

The IoT concept is based on connecting different and heterogeneous devices. This connection aims to make human life easier and more efficient, by automating some tasks and making communication faster and better especially in some important fields such as health service, industry, agriculture, transportation, education, or even our domestic daily life as shown in Figure 1. In smart homes, for example, we could switch on air conditioning before arriving home or unlock door for a visiting friend. We can even switch on or off light while we are kilometers away from home. With smart home applications, users can save time, energy, and money and win more life efficiency and comfort. Smart city surveillance, smart transportation, smart energy systems, smart water distribution, and security systems are all examples of IoT applications for smart cities. The collected data in the IoT environment would be analyzed in order to make right decisions at the right moments. However, in such systems, many challenges encounter the normal functioning, especially security challenge, which is by the way our focus in this paper. In fact, wireless mobile networks, which are the communication platform of IoT systems, are vulnerable to different security threats. These security risks can threaten the network in terms of confidentiality, integrity, availability, and other aspects. Thus, improving security and making these systems reliable become more and more mandatory in research field. Scientists and researchers are invited to perform studies in order to secure IoT especially in critical areas such as military domains or medical services. In addition, the IoT has raised public safety concerns, like cyberattacks and organized crimes which can be a serious risk for organizations and people's private life. In different places of the world, many serious attacks on IoT systems have been detected. On 27 June 2019, the US Food and Drug Administration (FDA) issued an alert about some insulin pumps manufactured by Medtronic that are vulnerable to be remotely accessed and controlled by hackers [1]. The same organization (FDA) confirmed, in 2017, that the implantable cardiac devices in St. Jude Medical could be easily hacked and controlled [2]. These devices are used to supervise patients' heart functioning and prevent or help in case of heart attacks. Nevertheless, hackers are able to access the device, control shocks, manage heartbeat, and give incorrect commands, due to some transmitter vulnerabilities. In April 2017, a malware named BrickerBot was discovered [3]. It attempted to definitively destroy IoT objects by executing harmful commands to delete their data and disable them. In

Figure 1: Example of communication domains in a smart environment.

2016, a certain hacker called Anna Senpai created a malware, called Mirai [4], which gains the access and take control of vulnerable connected objects such as routers and surveillance cameras, and create massive distributed denial of service attacks (DDos). Mirai transforms the infected objects into autonomous and intelligent bots controlled remotely. All these examples and many others show clearly that security issue is an urgent and crucial subject and its development is even more important than the development of IoT itself.

In our research, we focus on security requirement for mobile ad hoc networks (MANETs) which are widely used in IoT environments, thanks to their advantages like ease of implementation ease, being infrastructure-less, being self-organized, and dynamic topology. These advantages in terms of implementation and performance can also be seen as a weakness in terms of security and reliability, because of many factors, especially the lack of centralized infrastructure and the difficult implementation of control mechanisms. This character is our main motivation in this research. This paper is organized as follows: The next section presents some related studies in this security field. Section 3 will be dedicated to describing our architecture inspired from sharing a secret approach to secure communication in MANETs; this new algorithm is called Secure Protocol based on Identification, Detection, and Location and Isolation (SPIDLI) steps. This architecture provides a great solution against black hole, eavesdropping, and message tampering attacks. Section 4 is dedicated to discuss the schema example as a proof of concept. In Section 5, we will analyze some of the simulation results. The last section will conclude this paper.

2. Related Work

Complex network is based on graph theory and social sciences concepts and can be considered as a set of several connected nodes that interact in different ways [5]. The IoT concept is based on connecting different and heterogeneous devices [6]. The information exchanged in these networks varies according to the used context. It can be medical, military, agriculture, education, transport. or simply everyday home information [7]. Since this technology interacts with human activity especially in some sensitive domains, such as military or health service, it is necessary to guarantee that the shared information is highly secure [8].

Wang et al. in [9] presents a new metric called R_{NMI} to assess the robustness of the complex network based on standardized mutual information. Next, a simulated annealing algorithm is designed to reduce the damage. In order to improve the balance between attacks and errors, the authors propose a weighted metric to design connecting process R^{w}_{NMI} and a series of solutions focusing on attacks and errors.

Another study proposed by Wang and Liu in [10] focuses on resisting intentional attacks and cascading failures in complex networks, by proposing a framework called MAGA-NetR to improve the overall performance. This technique takes advantage of the fact that the robustness measures which evaluate the tolerance of the networks are not correlated with each other; therefore, this study proposes a standardized robustness measure R_n and this measure is validated to be effective in the experiments.

In order to facilitate the administration of public key certification, Shamir proposed the identity-based

cryptosystem approach in [11], and later, Boneh and Franklin concretized this approach using Weil coupling to provide an ID-based encryption scheme in [12]. As its name indicates, the ID-based cryptosystems are based on the identity information; therefore, each node in the network can use its identity as a public key instead of extracting it from a certificate generated by a certificate authority (CA) [13].

Shamir [14] and Blakley [15] are the first to introduce the notion of secret sharing scheme using (t, n) threshold. This scheme is based on two main steps as follows:

(i) Dividing step where the secret message is divided into n fragments, and then, each fragment is given to an authorized member

(ii) Rebuilding step where the collector tries to reconstruct the initial secret if and only if he combines at least k fragment received [16]

Zhou et al. proposed in [17] the combination between multipath routing and secret sharing to distribute the CA to multiple servers. Later, Kong et al. were interested in improving operations such as the signing of a certificate so that they can be done locally by the neighbors of the requesting node, distributing the servers more evenly over the network [18].

In the same context, and in order to diminish the effects of frequent topological changes, Tsirigos and Haas [19] proposed the application of concurrent multipath routing at the same time with diversity coding. Lou et al. [20] proposed a protocol named SPREAD to ensure data confidentiality and availability in order to strengthen network security. This method is based on four methods: directional transmission, controlling transmission power, shortest-distance routing, and controlling correlation factor. All concurrent multipath routes between any two nodes are considered in this method, but the limitation resides in the fact that active attacks cannot be detected. Through a multipath routing strategy, this protocol enhances the security and performance of an ad hoc network by providing an invented solution based on network coding techniques and the public key cryptosystem. This solution, however, assumes that a routing or multipath protocol is already implemented, so no study of specific routing algorithm has been carried out. In other words, SPREAD relies on multiple simultaneous paths between the source and the destination in MANET but cannot detect the positions of malicious nodes.

So our goal in this paper is not only to use multipath and secret sharing to improve availability and privacy but also to check the integrity of exchanged messages, in addition to locate the nodes suspected to be malicious.

2.1. System Model. Our architecture (totally invented by the author under patent N 42357 OMPIC, Casablanca, Morocco) is based on three essential steps to ensure *availability*, *confidentiality*, and *integrity*. These three steps are *Identification*, *Detection*, *Localization* and *Isolation* and come after a substep of initializing variables.

2.1.1. Initialization. This step is explained in Algorithm 1.

2.1.2. Identification. As described, the destination will receive r fragments of the message. Each combination of k fragments is a version of the message M. In this step (Figure 2), we will consider a metric called black hole coefficient (BH) that will be assigned to each node in the network based on its observed behavior during transmission. This coefficient will be initialized by 0 for all NEs and will be increased and decreased based on our own algorithm defined in the SPIDLI method as explained below. This coefficient will be used later to detect and isolate malicious nodes (Algorithm 2).

The destination can compare the reconstructed versions of the message using the following combination algorithm to ensure integrity.

Combination Algorithm. The total number of possible combinations is as follows:

$$C_r^k = \frac{A_r^k}{k!} = \begin{cases} 0, & \text{if } k > r, \\ \dfrac{r!}{k!\,(r-k)!}, & \text{if } 0 \le k \le r. \end{cases} \quad (1)$$

In practice, computing all combinations is a waste of time and resources. Thus, to optimize the computation process, we propose a minimal number α of combinations that sweep all received fragments. The idea to achieve this is to put $\alpha = \text{Roundup}(r/k)$ which is the next smallest integer that is larger than r/k. Let P_{rl} and P_{url} be the set of reliable paths and unreliable paths, respectively. Let C_{rl_i} be the reliable combination number i and C_{ssp_o} the suspicious combination number o $(1 \le i, o \le \alpha)$ (Algorithm 3).

So the equal combinations $C_{rl_i} (1 \le i \le \alpha)$ are correct combinations equal to the message M. Therefore, the fragments which constitute these reliable combinations are necessarily all reliable fragments $F_{rl_{i_j}}$ $(1 \le j \le k)$. And the different combinations $C_{ssp_o} (1 \le o \le \alpha)$ are suspect combinations constituted by suspicious fragments $F_{ssp_{o_t}} (1 \le t \le k)$; this is why our method will proceed to the second step to locate the unreliable fragments that have been modified during transmission generating different combinations.

2.1.3. Detection. Let F_{rl} (reliable fragments) be the set of fragments $F_{rl_{i_j}}$ $(1 \le i \le \alpha$ and $1 \le j \le k$ with $F_{rl_{i_j}} = F_{rl_{((i-1)k+j)}})$ which constitute equal and reliable combinations C_{rl_i} $(1 \le i \le \alpha)$. Let F_{ssp} (suspicious fragments) be the set of fragments $F_{ssp_{o_t}}$ $(1 \le o \le \alpha$ and $1 \le t \le k$ with $F_{ssp_{o_t}} = F_{ssp_{((o-1)k+t)}})$ which give different combinations C_{ssp_o} $(1 \le o \le \alpha)$ of suspect combination and then eliminate from F_{ssp} all the reliable fragments which belong to F_{rl} in order to have always $F_{rl} \cap F_{ssp} = \varnothing$.

In this step (Figure 3), we will consider a metric called unreliable coefficient (URL) that will be assigned to each node in the network based on its observed behavior during transmission. This coefficient will be initialized by 0 for all NEs and will be increased and decreased based on our own algorithm defined in the SPIDLI method as explained below. This coefficient will be used later to detect and isolate malicious nodes (Algorithm 4).

(i) **Step 1**: source node S marks n paths to the destination D. Let P_n be the set of paths between S and D. The value of n varies from one node to another according to the neighborhood of each node.
(ii) **Step 2**: S divides the message M using Shamir secret sharing scheme to n fragments $\{F_1, F_2, \ldots, F_n\}$
(iii) **Step 3**: the source then chooses one threshold k of the Shamir method $(k \leq n)$, k also varies according to n and the number of the node-disjoint paths
(iv) **Step 4**: S encapsulates each fragment F_i in a packet and then sends it in a path P_i from P_n.
(v) **Step 5**: the destination D receives r packets $(r \leq n)$. Let P_r be the set of paths where D received r packets.
(vi) **Step 6**: S receives r acknowledgments; let us suppose that a path is bidirectionally trusted/untrusted.

Algorithm 1: Initialization steps.

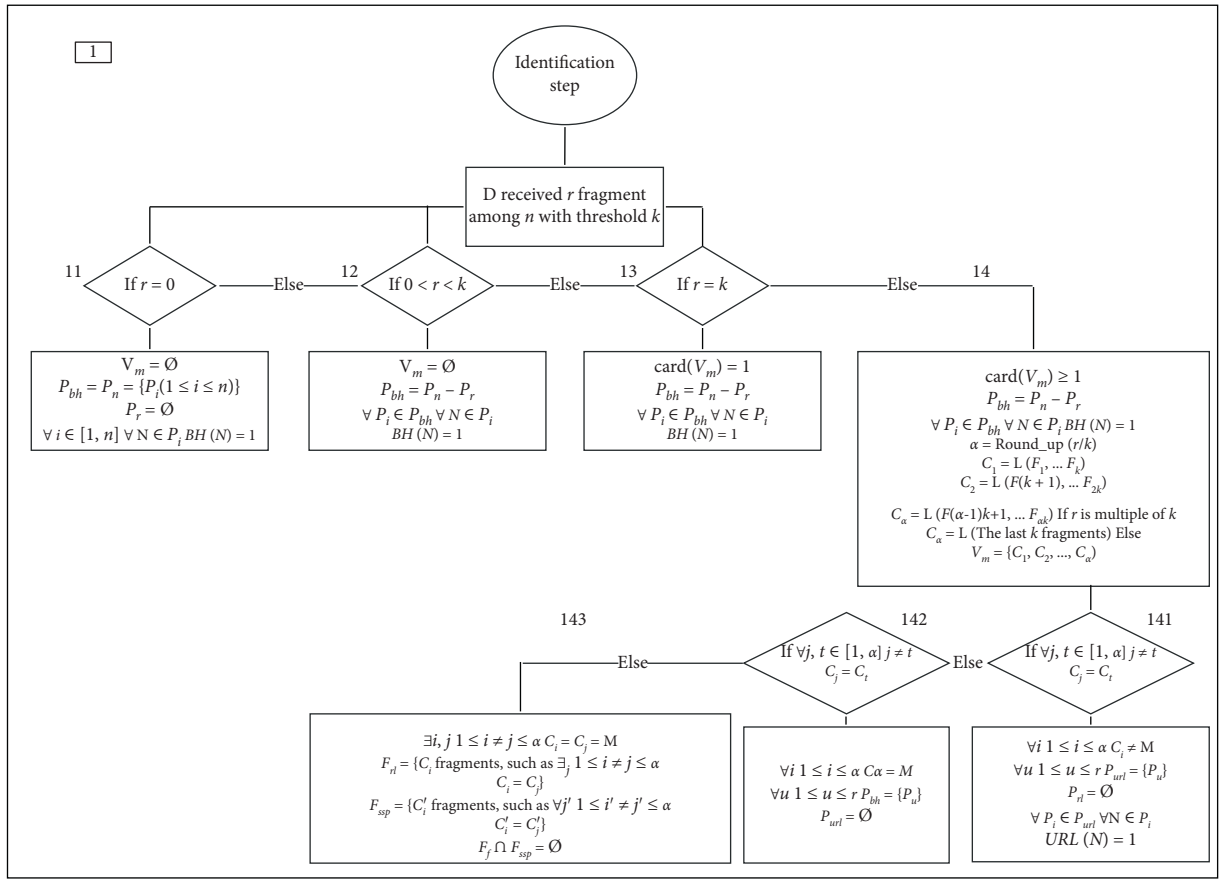

Figure 2: Organizational chart of identification step.

Step 1: in this step, destination D reconstructs the message M from the received fragments. Let V_m be the set of all possible versions of M. Let us discuss the possible scenarios:

(i) **If** $0 \leq r < k$, the destination cannot reconstruct the message M sent by S; $V_m = \varnothing$. The source resends the missing fragments in the paths where the acknowledgments are received. In order to optimize the process for future transmission, the source returns to the initialization step and recalculates n and k so that n becomes equal to r. Let P_{bh} be the set of paths that may contain black holes. In the case $P_{bh} = P_n - P_r$, the source S assigns the value 1 to the black hole coefficient to all the nodes that constitute these paths. $\forall P_i \in P_{bh}$, $\forall N \in P_i$, $BH(N) = 1$
(ii) **If** $r = k$, the destination D can reconstruct one version of the message M using the Shamir method. In the case card $(V_m) = 1$ and $P_{bh} = P_n - P_r$, the source S assigns the value 1 to the black hole coefficient to all the nodes that constitute these paths. $\forall P_i \in P_{bh}$, $\forall N \in P_i$, $BH(N) = 1$
(iii) **If** $k + 1 \leq r \leq n$, the destination, using Lagrange polynomial (Shamir method), can reconstruct many versions of the message. The associated Lagrange polynomial is written as follows:
$L(0) = \sum_{j=0}^{k-1} f(x_j) \prod_{m=0, m \neq j}^{k-1} x_m / (x_m - x_j)$

Algorithm 2: Identification steps.

Step 1: destination calculates the possible combinations that cover all the elements of our set $\{F_1, F_2, \ldots F_r\}$

$C_1 = L(F_1, \ldots F_k)$

$C_2 = L(F_{k+1}, \ldots F_{2k})$

$C_3 = L(F_{2k+1}, \ldots F_{3k})$

...

$$C_\alpha = \begin{cases} L(F_{(\alpha-1)k+1}, \ldots, F\alpha k), & \text{if, } r \text{ is multiple of } k \\ L(\text{The last } k \text{ fragments}), & \text{else} \end{cases}$$

$V_m = \{C_1, C_2, \ldots, C_\alpha\}$

(i) **If** $\forall i, j \in \{1, \alpha\}\ C_i = C_j$:
So all the paths $P_j\ 1 \le j \le r$ are reliable paths, and the initial message sent by the source is equal to C_i,
$\forall i,\ 1 \le i \le \alpha,\ C_i = M,\ P_{url} = \varnothing,\ P_{rl} = \{P_1, P_2, \ldots, P_r\}$

(ii) **If** there are different combinations, and at least two equal combinations: So the equal combinations C_{rli} $(1 \le i \le \alpha)$ are correct combinations equal to the message M. Therefore, the fragments which constitute these reliable combinations are necessarily all reliable fragments F_{rlij} $(1 \le j \le k)$. And the different combinations C_{ssp_o} are suspect combinations constituted by suspicious fragments F_{sspot} $(1 \le t \le k)$, that is why our method will proceed to the second step to locate the unreliable fragments that have been modified during transmission generating different combinations.

Algorithm 3: Combination algorithm.

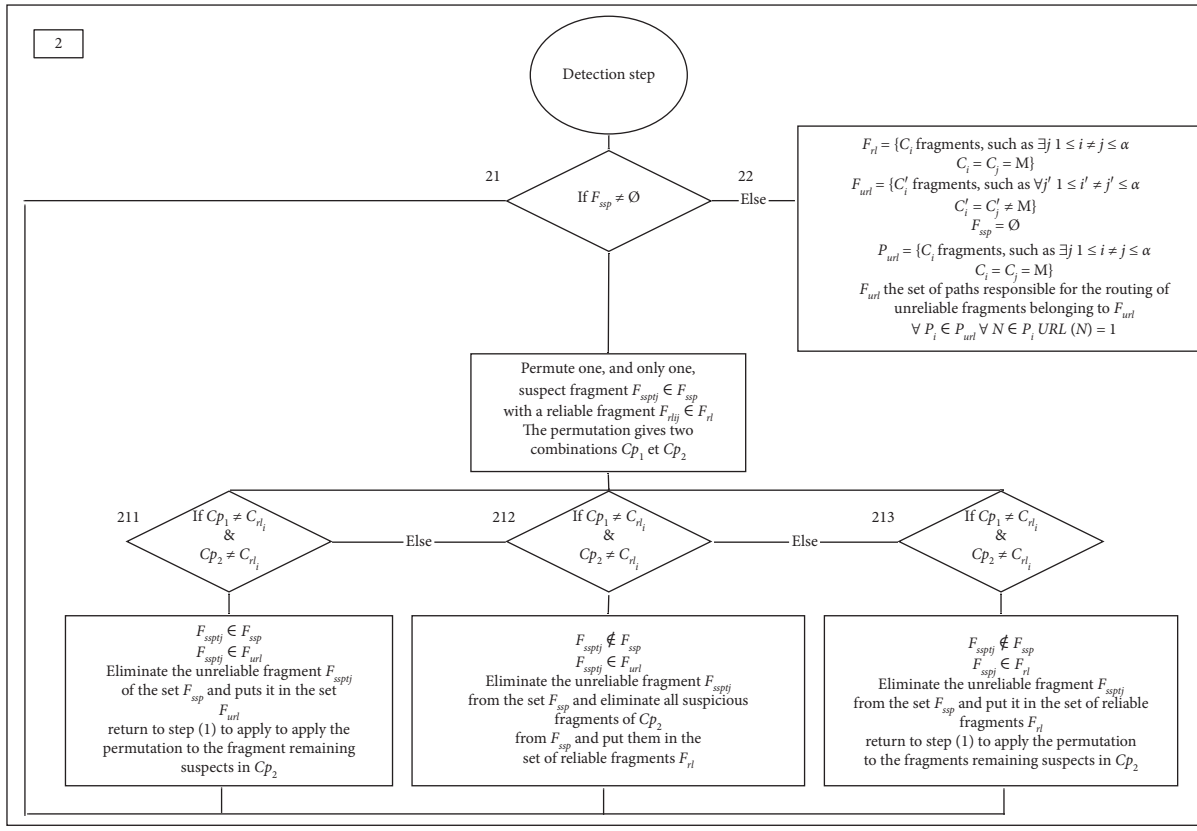

Figure 3: Organizational chart of detection step.

2.1.4. Location and Isolation. In this step (Figure 4), broadcasting the information of the coefficients obtained in the previous steps allows the network to identify and locate black holes and unreliable nodes (Algorithm 5).

Proof of Concept. Let $n = 12$, $k = 4$, and $r = 11$ as shown in Figure 5.

The source divides the message M on $n = 12$ fragments, $F'_1, \ldots F'_{12}$, with a threshold $k = 4$ and sends each fragment F_i in a path P_i (Figure 5):

$$P_n = \{P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8, P_9, P_{10}, P_{11}, P_{12}\}. \quad (2)$$

The destination receives $r = 11$ fragments, $F_1, F_2, .., F_{11}$:

Begin

Step 1: the destination performs permutations of one, and only one, suspect fragment $F_{sspo_j} \in F_{ssp}$, with a reliable fragment $F_{rl_{i_j}} \in F_{rl}$. The permutation gives two combinations

$C_{p_1} = L(F_{rl_{i_1}}, \ldots, F_{ssp_{o_j}}, \ldots, F_{rl_{i_k}})$

$C_{p_2} = L(F_{ssp_{o_1}}, \ldots, F_{rl_{i_j}}, \ldots, F_{ssp_{o_k}})$, $1 \le i, o \le \alpha$

Step 2: each time, the destination compares the computed combinations C_{p_1} and C_{p_2} with one of the reliable combinations C_{rl_i} so

(i) **If** $C_{p_1} \neq C_{rl_i}$ and $C_{p_2} \neq C_{rl_i}, F_{ssp_{o_j}}$ is an unreliable fragment, because it gives an incorrect combination with a set of only reliable fragments. The destination, thus, updates the two sets F_{url} and F_{ssp}; it eliminates the unreliable fragment $F_{ssp_{o_j}}$ from the set F_{ssp} and puts it in the set F_{url}; it returns to step (1) to apply the permutation to the fragments remaining suspects in C_{p_2}.

(ii) **If** $C_{p_1} \neq C_{rl_i}$ and $C_{p_2} = C_{rl_i}, F_{ssp_{o_j}}$ is an unreliable fragment and all C_{p_2} fragments are reliable fragments The destination, thus, updates the sets F_{rl}, F_{url}, and F_{ssp}; it eliminates the unreliable fragment $F_{ssp_{o_j}}$ from the set F_{ssp} and put it in the set of unreliable fragments F_{url}, and it eliminates all suspicious fragments of C_{p_2} from F_{ssp} and put them in the set of reliable fragments F_{rl}.

(iii) **If** $C_{p_1} = C_{rl_i}$ and $C_{p_2} \neq C_{rl_i}, F_{ssp_{o_j}}$ is a reliable fragment, because it gives a correct combination with a set of only reliable fragments. The destination, thus, updates the two sets F_{rl} and F_{ssp}; it eliminates the unreliable fragment $F_{ssp_{o_j}}$ from the set F_{ssp} and puts it in the set F_{rl}; it returns to step (1) to apply the permutation to the fragments remaining suspects in C_{p_2}.

Step 3: D checks if all suspicious fragments of F_{ssp} are swept until $F_{ssp} = \varnothing$.

Step 4: In all previous cases, $P_{bh} = P_n - P_r$; the source S assigns the value 1 to the black hole coefficient to all the nodes that constitute these paths.

$\forall P_i \in P_{bh}$, $\forall N \in P_i$, $BH(N) = 1$

The destination D assigns also the value 1 to the coefficient of unreliability URL to all the nodes which constitute the unreliable paths P_{url}. Then, S and D exchange this information.

$\forall P_j \in P_{url}$, $\forall N \in P_j$, $URL(N) = 1$

END

Algorithm 4: Detection steps.

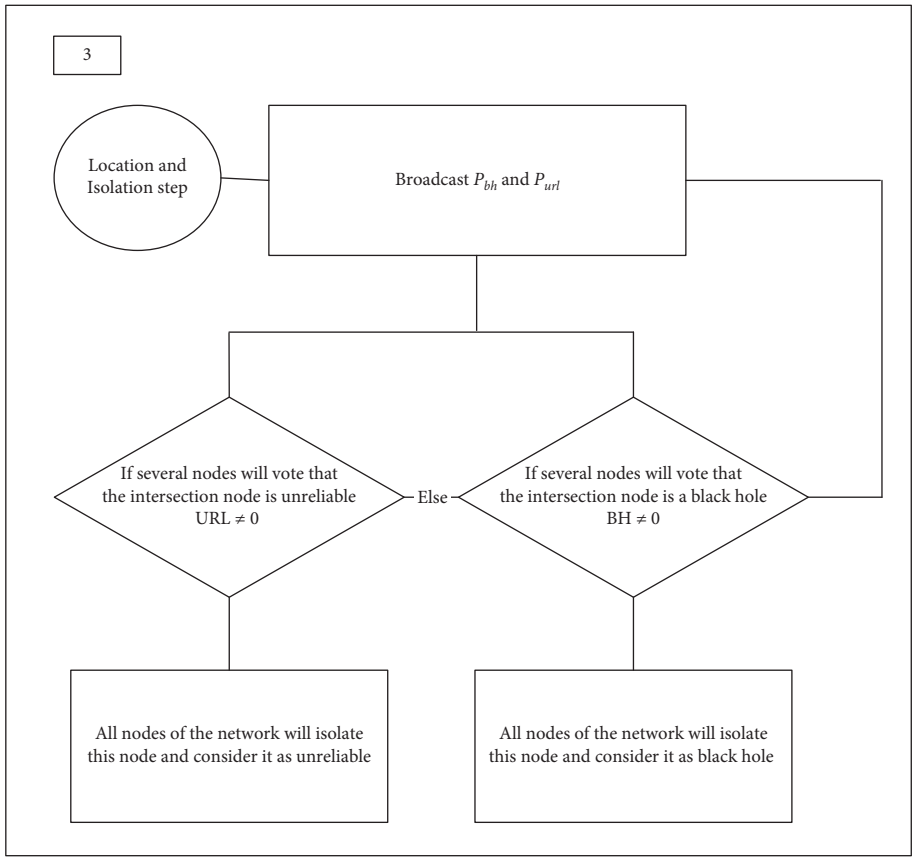

Figure 4: Organizational chart of location and isolation step.

Begin
Step 1: as long as there are intersections between paths containing black holes, several nodes will vote that the intersection node is a black hole; then, its $BH \neq 0$ and BH is higher than a specified threshold that will be fixed in advance. So all the nodes of the network will isolate this node and consider it as black hole.
Step 2: by the same process, the nodes suspected to be unreliable will be located and isolated too.
We initialize at all nodes of the network the coefficients black hole BH and unreliable URL to 0
$\forall$ N is the node of the network $BH\ (N) = 0$ and $URL\ (N) = 0$
END

Algorithm 5: Location and isolation steps.

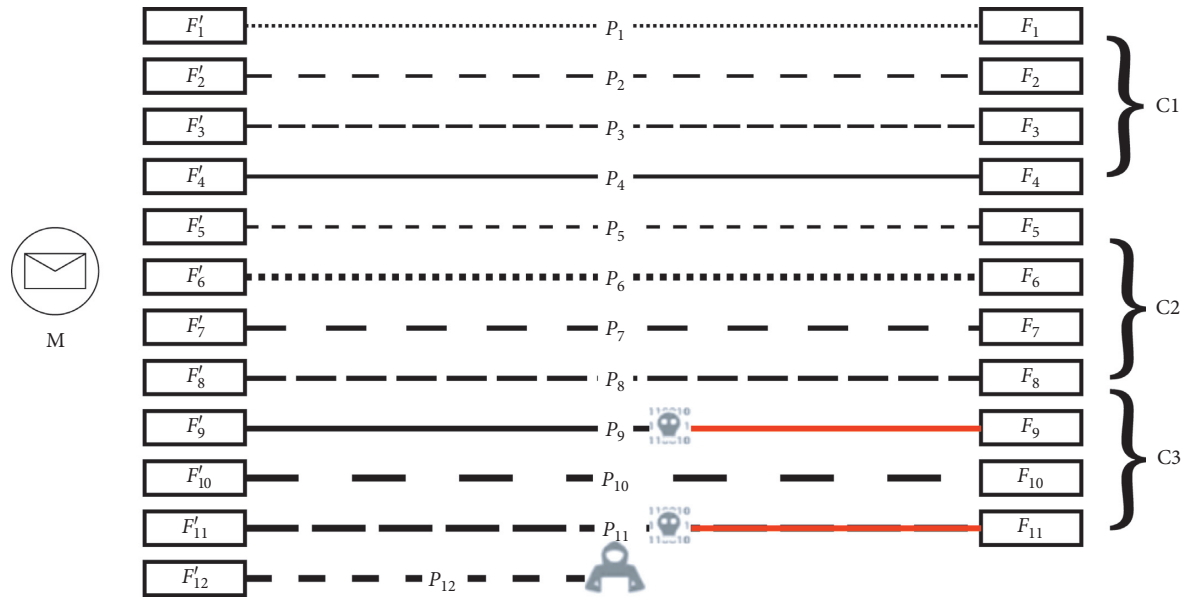

Figure 5: Example scenario of the SPIDLI protocol.

$$
\begin{aligned}
P_r &= \{P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8, P_9, P_{10}, P_{11}\},\\
\alpha &= \text{roundup}\left(\frac{r}{k}\right),\\
C_1 &= L(F_1, F_2, F_3, F_4),\\
C_2 &= L(F_5, F_6, F_7, F_8),\\
C_3 &= L(F_8, F_9, F_{10}, F_{11}),
\end{aligned}
\tag{3}
$$

where C_1 and C_2 are two correct combinations equal to the original message M sent by the source, but the combination C_3 is not correct. Then,

$$
\begin{aligned}
F_{rl} &= \{F_1, F_2, F_3, F_4, F_5, F_6, F_7, F_8\},\\
F_{ssp} &= \{F_8, F_9, F_{10}, F_{11}\},\\
F_{url} &= \varnothing.
\end{aligned}
\tag{4}
$$

Since $F_8 \in F_{rl}$, $F_{ssp} = \{F_9, F_{10}, F_{11}\}$.

Swap F_9 from incorrect combination C_3 with F_2 from the correct combination C_1:

$$
\begin{aligned}
C_1 &= L(F_1, F_2, F_3, F_4),\\
C_{p_1} &= L(F_1, F_9, F_3, F_4),\\
C_3 &= L(F_8, F_9, F_{10}, F_{11}),\\
C'_{p_1} &= L(F_8, F_2, F_{10}, F_{11}).
\end{aligned}
\tag{5}
$$

$C_{p_1} \neq C_1$. So we are sure that the fragment F_9 was modified during the transmission.

So, $F_{rl} = \{F_1, F_2, F_3, F_4, F_5, F_6, F_7, F_8\}$, $F_{url} = \{F_9\}$, and $F_{ssp} = \{F_{10}, F_{11}\}$.

$C'_{p_1} \neq C_1$. So we are not sure if two fragments F_{10} and F_{11} are both unreliable or one of them; therefore, we will repeat another permutation of F_{10} of the new combination C'_{p_1} with F_3 of C_1:

$$
\begin{aligned}
C_1 &= L(F_1, F_2, F_3, F_4),\\
C_{p_2} &= L(F_1, F_2, F_{10}, F_4),\\
C'_{p_1} &= L(F_8, F_2, F_{10}, F_{11}),\\
C'_{p_2} &= L(F_8, F_2, F_3, F_{11}).
\end{aligned}
\tag{6}
$$

Table 1: Parameters value.

Parameter	Value
Routing protocol	SPIDLI/MPOLSR
Simulation time	250 seconds
Number of nodes	10, 20, 30, 40, 50, 60, 70, 80, 90, and 100 nodes
Environment area	1000 meter × 1000 meter
MAC protocol	IEEE 802.11
Transport layer	Transmission control protocol (TCP)
Maximum speeds	5 meter/second
Mobility model	Random waypoint

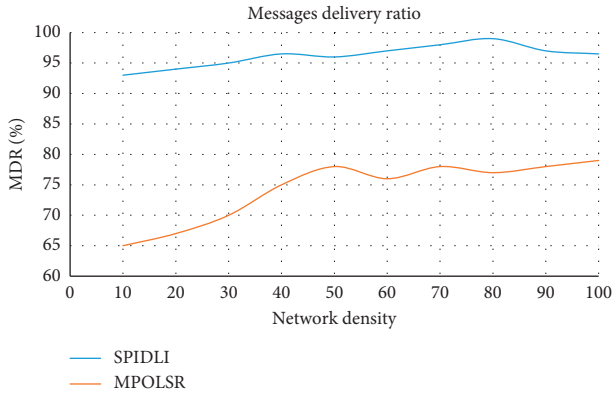

Figure 6: Message delivery ratio graph.

$C_{p_2} = C_1$. So we are sure that the fragment F_{10} was not modified during the transmission; thus, F_{10} is correct.

Then, $F_{rl} = \{F_1, F_2, F_3, F_4, F_5, F_6, F_7, F_8, F_{10}\}$, $F_{url} = \{F_9\}$, and $F_{ssp} = \{F_{11}\}$.

$C'_{p_2} \neq C_1$. So we are sure that the fragment F_{11} has been modified during the transmission.

Then, $F_{rl} = \{F_1, F_2, F_3, F_4, F_5, F_6, F_7, F_8, F_{10}\}$, $F_{url} = \{F_9, F_{11}\}$, and $F_{ssp} = \varnothing$. □

3. Analytical Results

In order to evaluate our protocol SPIDLI, and their impact on network performances, we have implemented a simulation in the NS2 platform with the objective of evaluating the efficiency of our solution. We have compared our method with standard MPOLSR in a medium size ad hoc network under a random black hole attack. The used parameters are shown in Table 1:

In this simulation, we will observe three main metrics: MDR (message delivery ratio), end-to-end delay, and throughput. We will compare the standard MPOLSR and SPIDLI. We used in our simulation the MPOLSR type which is based on load sharing.

Figure 6 shows the evolution of message delivery ratio with network density in both MPOLSR and SPIDLI in case of a black hole attack average of 20% of nodes number. The simulation result shows clearly that our method improves the MDR comparing with standard MPOLSR. The objective of SPIDLI is to increase the chance of a message to reach the destination node. This objective is achieved according to the

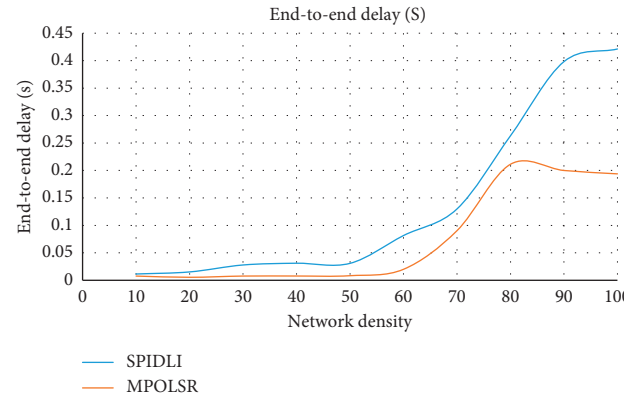

Figure 7: End-to-end delay graph.

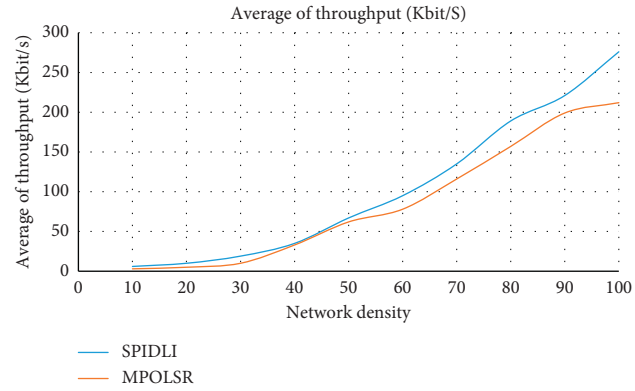

Figure 8: Throughput graph.

simulation result. We can observe also that the MDR increases with network density, which is explained by the fact that having a high number of nodes gives more available routes (high threshold k) to reroute the message from the source to destination.

In this graph (Figure 7), we analyze the average delay evolution according to network density for MPOLSR and SPIDLI protocols with black hole attack. When network density is relatively small, the number of paths in SPIDLI is nearly the same as MPOLSR; thus the threshold k is smaller (equal to 1 or 2). As a result, the calculation processing does not impact the end-to-end delay. However, when the density becomes higher, we observe that the end-to-end delay increases specially in case of SPIDLI. This can be justified by the fact that each node performs extra processing for x or calculation and queuing operations in order to reconstruct the initial message. In addition, the paths selected using SPIDLI may be longer than those selected using standard MPOLSR, which may also generate more delay.

In Figure 8 we analyze the evolution of average throughput in function of network density in a simulation of mobile networks with attacks of both MPOLSR and SPIDLI. We can see that throughput in case of SPIDLI is slightly higher than MPOLSR in a network with more than 50 nodes. This behavior can be explained by the fact that SPIDLI generates extra packets more than MPOLSR. In addition, the

dropped packets in MPOLSR are retransmitted which affects the throughput.

4. Conclusion

As conclusion, with the emerging IoT and smart cities, the security aspect becomes more and more insisting and research and studies are highly recommended. In this context, we have invented a new method named SPIDLI where we provide a scheme aiming to prevent some security threats especially black holes, message tampering, and eavesdropping attacks putting at risk the availability, integrity, and confidentiality (respectively) of data in ad hoc networks. This security prevention is mandatory in some cases of IoT where the exchanged information is sensitive and confidential. We have implemented our solution in the NS2 simulation environment to compare it with the standard MPOLSR protocol and found some considerable results. As future work, we will try to optimize our solution to enhance the performance in terms of end-to-end delay and evaluate other important KPIs such as energy consumption and jitter.

Data Availability

No data were used to support this study.

Conflicts of Interest

All the authors have read the manuscript and have approved this submission. The authors report no conflicts of interest.

References

[1] Medtronic. Cybersecurity notice-legacy exchange program, 2019.

[2] CNN Business, *Fda Confirms that St. Jude's Cardiac Devices Can Be Hacked*, CNN Business, Atlanta, GA, USA, 2017.

[3] D. Goodin, "Brickerbot, the permanent denial-of-service botnet, is back with a vengeance," *Ars Technica*, 2017.

[4] J. Biggs, *Hackers Release Source Code for a Powerful Ddos App Called Mirai*, Vol. 19, TechCrunch, San Francisco Bay Area, CA, USA, 2016.

[5] J. Yan, H. He, and Y. Sun, "Integrated security analysis on cascading failure in complex networks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 3, pp. 451–463, 2014.

[6] F. El Mahdi, B. Bouamoud, and H. Ahmed, "Analyzing security in smart cities networking and implementing link quality metric," in *Proceedings of the 2019 Third International Conference on Intelligent Computing in Data Sciences (ICDS)*, pp. 1–8, IEEE, Marrakech, Morocco, October 2019.

[7] F. El Mahdi, H. Ahmed, M. Nada, and B. Essaid, "Study of security in manets and evaluation of network performance using etx metric," in *Proceedings of the 2017 International Conference on Smart Digital Environment*, pp. 220–228, ACM, Rabat, Morocco, July 2017.

[8] F. El Mahdi, H. Ahmed, B. Bouamoud, and M. Souidi, "Bootstrapping services availability through multipath routing for enhanced security in urban iot," in *Proceedings of the 4th International Conference on Smart City Applications*, pp. 1–9, Casablanca, Morocco, October 2019.

[9] S. Wang, J. Liu, and X. Wang, "Mitigation of attacks and errors on community structure in complex networks," *Journal of Statistical Mechanics: Theory and Experiment*, vol. 2017, no. 4, Article ID 043405, 2017.

[10] S. Wang and J. Liu, "Designing comprehensively robust networks against intentional attacks and cascading failures," *Information Sciences*, vol. 478, pp. 125–140, 2019.

[11] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques*, pp. 47–53, Springer, Davos, Switzerland, May 1984.

[12] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology-CRYPTO 2001*, pp. 213–229, Springer, Berlin, Germany, 2001.

[13] Z. Hui, C. Li-Qing, and Q.-Y. Zhu, "The application of threshold secret sharing in key agreement scheme for manets," in *Proceedings of the 2012 International Conference on Computer Science and Service System*, pp. 837–840, IEEE, Nanjing, China, August 2012.

[14] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, 1979.

[15] G. R. Blakley, "Safeguarding cryptographic keys," in *Proceedings of the 1979 International Workshop on Managing Requirements Knowledge (MARK)*, vol. 48, New York, NY, USA, June 1979.

[16] S. Chen and M. Wu, "Secure multipath routing based on secret sharing in mobile ad hoc networks," in *Proceedings of the 2009 IEEE International Conference on Network Infrastructure and Digital Content*, pp. 539–542, IEEE, Beijing, China, November 2009.

[17] L. Zhou and Z. J. Haas, "Securing ad hoc networks," *IEEE Network*, vol. 13, no. 6, pp. 24–30, 1999.

[18] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing robust and ubiquitous security support for mobile ad hoc networks," in *Proceedings of the Ninth International Conference on Network Protocols. ICNP 2001*, vol. 1, pp. 251–260, Citeseer, Riverside, CA, USA, November 2001.

[19] A. Tsirigos and Z. J. Haas, "Analysis of multipath routing, part 2: mitigation of the effects of frequently changing network topologies," *IEEE Transactions on Wireless Communications*, vol. 3, no. 2, pp. 500–511, 2004.

[20] W. Lou, W. Liu, Y. Zhang, and Y. Fang, "Spread: improving network security by multipath routing in mobile ad hoc networks," *Wireless Networks*, vol. 15, no. 3, pp. 279–294, 2009.