future internet

MDPI

Article

An Image Hashing-Based Authentication and Secure Group Communication Scheme for IoT-Enabled MANETs

Aiiad Albeshri

Department of Computer Science, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 80221, Saudi Arabia; aaalbeshri@kau.edu.sa

Abstract: Mobile ad hoc networks (MANETs) play a highly significant role in the Internet of Things (IoT) for managing node mobility. MANET opens the pathway for different IoT-based communication systems with effective abilities for a variety of applications in several domains. In IoT-based systems, it provides the self-formation and self-connection of networks. A key advantage of MANETs is that any device or node can freely join or leave the network; however, this makes the networks and applications vulnerable to security attacks. Thus, authentication plays an essential role in protecting the network or system from several security attacks. Consequently, secure communication is an important prerequisite for nodes in MANETs. The main problem is that the node moving from one group to another may be attacked on the way by misleading the device to join the neighboring group. To address this, in this paper, we present an authentication mechanism based on image hashing where the network administrator allows the crosschecking of the identity image of a soldier (i.e., a node) in the joining group. We propose the node joining and node migration algorithms where authentication is involved to ensure secure identification. The simulation tool NS-2 is employed to conduct extensive simulations for extracting the results from the trace files. The results demonstrate the effectiveness of the proposed scheme based on the memory storage communication overhead and computational cost. In our scheme, the attack can be detected effectively and also provides a highly robust assurance.

Keywords: MANET; node mobility; secure communication; image hashing; clustered deployments

Citation: Albeshri, A. An Image Hashing-Based Authentication and Secure Group Communication Scheme for IoT-Enabled MANETs. *Future Internet* **2021**, *13*, 166. https://doi.org/10.3390/fi13070166

Academic Editor: Paolo Bellavista

Received: 10 June 2021
Accepted: 25 June 2021
Published: 27 June 2021

1. Introduction

The Internet of Things (IoT) involves multifaceted communication across different networks. These networks include sensing devices; automobiles; household appliances; devices based on sensors, electronics, and software connections. With seamless connectivity between devices and rapid information exchange, this concept provides advanced services that are available, regardless of the time, space, and person. The IoT can include various wireless networks and mobile ad hoc networks (MANETs). The deployment of IoT devices has increased significantly in recent years for buildings (houses, schools, factories, and offices), transportation, automobiles, and health organizations [1].

MANETs consist of several mobile nodes that connect to or leave during the operations of the intended network. In large communication networks, image hashing-based authentication provides resilience against several security attacks. Existing routing studies include obstacles and methods based on control [1]. The integration of MANETs and the IoT forms a developing paradigm to allow communication among smart devices in the IoT. Furthermore, the weak infrastructure increases the chances of security attacks by the malicious nodes that compromise confidential information. Thus, in MANET–IoT, security against strong competitors is still difficult [2]. MANET is a low-cost, dynamic, and distributed network with self-adjusting capabilities [3,4]. It consists of a cluster of mobile nodes that establish the communication opportunistically. MANET follows the architecture of infrastructure at a centralized station or rolling mill. Specific features of MANET include

the following: dynamic topology, multi-hop communication, decentralization infrastructure, scalability, and short connection. The rapid development of wireless technology increases the current demand for IoT [5]. The IoT can be described as a network made up of millions of different devices that allow intelligent "stuff" in between. The expansion of opportunistic communication is noticeable in IoT devices, as they are associated with dynamic devices and integrated with IoT enabling adaptable communication between IoT MANET devices [6]. The introduction of MANET into the IoT facilitates improved connectivity through multi-hop connectivity and also supports high scaling. With the integration of MANET, IoT applications can be deployed in military scenarios, smart city applications, waste management, and disaster management, etc. However, the lack of infrastructure and centralized controls increases the risk for the MANET–IoT environment. MANET is susceptible to security attacks, e.g., jamming, Black-hole attack, Sibyl attacks, and packet dropping attacks. These attacks slow down the whole network [7,8]. MANET is more vulnerable to attacks compared to the networks based on infrastructure. Creating a secure MANET connection is difficult due to: (1) a public wireless device, (2) an unclear defense line, (3) a self-regulatory and self-motivated network, (4) a large number of broadcast messages, (5) hop-by-hop messages, and 6) limited nodes' charge and capacity of batteries [2].

Trust is initiated from the sociology domain [3]. Trust plays a vital role in enhancing the security of specialized networks by a priori assessments or by evaluating the trust of their peers before making any route decisions. Due to resource constraints (e.g., power and bandwidth), not all nodes can participate in the routing and then send packets. Node reliability is a good measure to guarantee the accessibility of the nodes and to ensure reliable communication between them [4]. The mechanisms of cryptography cannot assist in the sensing/blocking of such network-based accidental threats. The trust management concept does not interchange cryptography; however, it improves it. The cryptography and credentials framework decision work manually to achieve the security of MANET-IoT. To provide consistent, protected, and well-timed network packages, this work is based on a cluster in MANET-IoT [5]. The MANET-IoTnodes were grouped into single clusters [6], and a predictive model based on trust management was established to calculate and distribute trust. Moreover, an ideal model for identifying malicious nodes and progressing network functioning was also established.

The main problem addressed in the paper is the mobility of the nodes. Therefore, a node is out of the group and wants to join another group so it can be easily attacked from the middle. Attackers can now easily find the device and link the cluster with official approval. The group head (GH) should not permit the pairing of soldiers and devices that are attacker nodes. This paper presents an efficient authentication scheme based on image hashing (IHA) to provide the secure joining and mobility of nodes in the network. In the system model, asymmetric keys are utilized for secure communication in the network. GHs and the network administrator (NA) collaborate to authenticate the node based on security credentials and image hashing. The main contributions of this paper are as follows:

1. We evaluated the literature and identified the research from recent and related schemes.
2. An image hashing-based authentication scheme is proposed to migrate the nodes to other groups securely. Asymmetric keys were employed for secure communication.
3. The proposed image hashing-based node joining and migration mechanisms are presented. These mechanisms provide secure mobility of the node within the network.
4. Finally, extensive simulations were conducted to extract the results from trace files.

The rest of the paper is organized as follows: Section 2 provides a review of the existing and related literature; Section 3 demonstrates our system model; Section 4 presents the proposed work; Section 5 provides the results and analysis; finally, Section 6 concludes the paper.

2. Related Work

MANET has been widely explored over the last decade. In recent years, the explosion of the Internet has significantly increased the use and benefits of MANET. MANET-IoT is an important and emerging concept, as wireless devices are self-connected and self-organized. The safety and consistency necessities of this kind of network should, therefore, be re-examined. Regarding next-generation computing, in the IoT, MANET is expected to be a significant key player. A smart concept of MANET in 5G is presented by Tanveer in [9]. A robust image hashing scheme provides efficient authentication. The dominant coefficients are employed to minimize the computational cost. A novel approach is applied for image hashing-based authentication. Moreover, this scheme provides secure data transmission over the network. [10].

An image hashing-based scheme provides multiple attack detection and adaptive thresholding for image authentication. A hashing algorithm is applied to the image to extract hash values for authentication [11]. Waleed proposed a new predictive trust-based model for MANET in the IoT [12] that calculates the final node value based on direct and indirect opinions of trust. A secure routing protocol is also designed to transfer the data packets securely. Numerous protocols of routing based on trust were proposed and appraised in an ad hoc network development. Most trust management plans are created for joint routing to identify the wrong nodes that are self-destructive or harmful. When designing safer route protocols, researchers have adopted reputational associations concerning mobile nodes. In [13], Desai et al. presented a predictive route model that numerically identifies different security attacks. In [14], Rath et al. explained the key security problems for the IoT in MANET. They concentrated on security and vulnerability threats for ad hoc networks and the creation of a comprehensive flight network using the IoT. Riyaz et al. proposed a scheme in MANET based on routing protocols [15]. In this approach, protocols of routing are employed to transfer the data packets to the concerned destination in MANET. An effective approach based on the triple factor is used to transmit the data into a secure path. K. Dhanya et al. [16] presented a proposal based on secure autonomic MANET in a trusted routing path. This research work is based on trust using routing protocols in MANET. Moreover, several surveys and various approaches are presented from the perspective of MANET. F. Khan [17] presented a scheme based on secure communication for IoT-based networks in MANET. In his research work, the quality of services (QoS) can be improved using existing resources that enhance the performance of a network.

H. Y. Zhao et al. [18] presented an energy consumption scheme based on an ant colony for MANET-IoT. A novel algorithm has been proposed for node computing and the joining and disjoining of nodes in the transmission route of energy consumption in IoT–MANET. Moreover, a novel ant colony architecture is presented in which nodes join a greedy approach that massively shortens the run-time. M. A. Saleem [19] proposed a routing scheme based on group routing for the framework of data clusters to obtain the optimal route. He also explored the conventional standards of MANET and VANET (Vehicular Ad Hoc Network) and their behaviors in smart cities. In [20], a novel approach using a fluctuating topology for securing the exchange key is presented. He used a MANET-based advanced model and designed a key exchange scheme. This scheme shortened the attacker's accessibility. Degan Zhang et al. [21] proposed an approach with trust matrices by using an adaptive approach. This method calculates the trust by using data packets. The proposed approach successfully protects the data from attackers. Burhan ul Islam Khan [22] designed an efficient model based on computation to enhance security. As security is a key issue in MANET and the secure transmission of data is more crucial in recent years, several efficient solutions are proposed in his research to overcome these security issues. A game-based model is presented that detects different security attacks and secures all nodes. Rashidah et al. [23] proposed a security-based model for MANETs. This model has analyzed the performance and behavior of nodes and the reputation of the system simultaneously. Moreover, results show that the system's performance has significantly

improved, and throughput has been enhanced. S. N. Mohammad et al. [24] presented a novel security architecture, ESMBMCRT. Security is enhanced to protect against black hole attacks and reduces energy consumption.

Nguyen proposed a scheme based on an asymmetric key for the classification and verification of a large-scale MANET [25]. The team leader issues certificates to all nodes. Each node provides the certificate without the assistance of any authority of trusted certification. Moreover, this scheme reduces network consumption and increases network deployment. Team leaders have membership nodes, and other team members can communicate with one another. As shown in Figure 1, the sender transmits the image hash to the receiver node by encrypting it with the public key of the receiver node. The receiving node decrypts the received image by using its private key. Vincent and Pushpa have proposed a structured approach of key management; [26] the cluster head (CH) is selected for a group that contains the ultimate value of reliability. To calculate public and private keys for nodes, private key generation (PKG) has been utilized widely. The NA chooses the CH after the election, and the CA's offline limit is set to request a new node to connect to the network. The agent mobile is the segment of an application that obtains confidential data from several trusted network nodes and also information of nodes that the certificates have passed. SRIH [27], a secure and robust image hashing-based scheme, employs a Gaussian pyramid. Key-based encryption is utilized to secure the hash, and authentication is conducted based on image hashing. This scheme detects different malicious attacks and also provides resilience against malicious attacks. ESIH [28], an efficient and secure image hashing-based authentication scheme, is utilized with an improved design. Sufficient time must be provided for efficient authentication and verification.

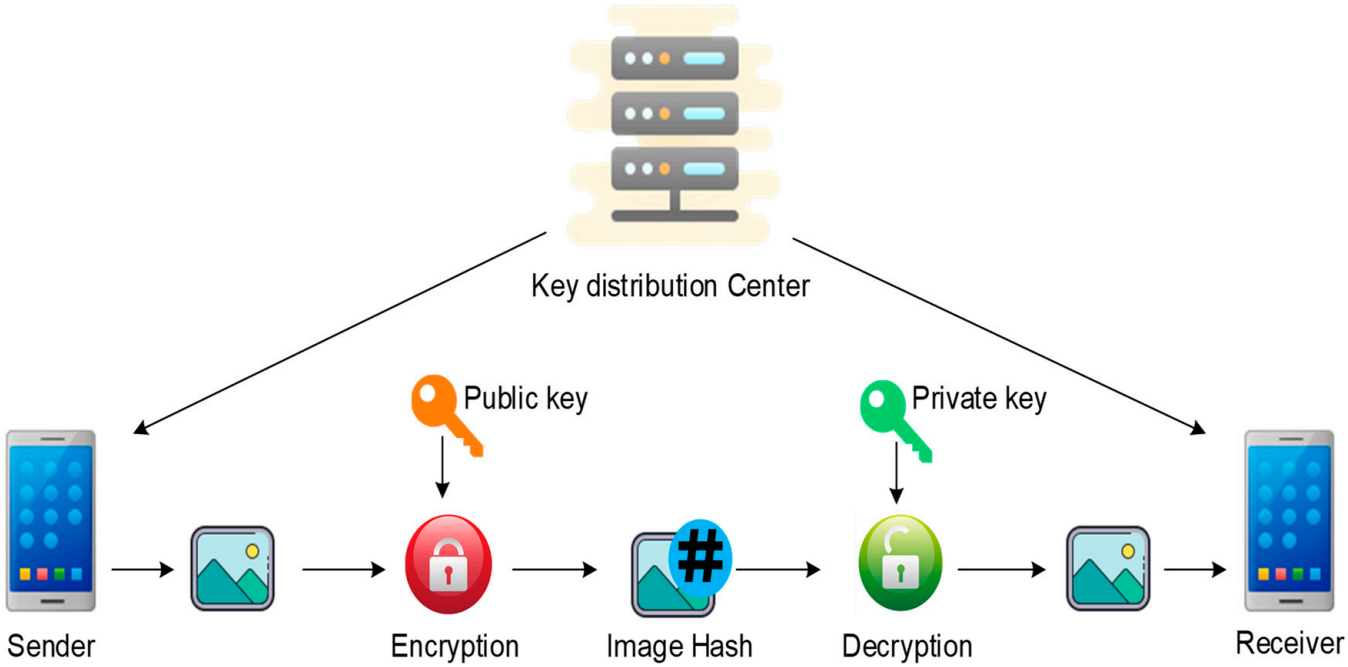


Figure 1. Public-key distribution scenario with image hash [26].

This plan has the following benefits: the node generates a public key based on a similar (n) origin and CA assigned to its node ID. Each node has a public key of self-disconnection, known as a cluster. Therefore, the cluster nodes do not press their public keys on all adjacent nodes, which occupy less of the network storage space and bandwidth simultaneously. The CH public key changes at times, and each CH compares its new public key against the value of the trust and the previous (larger) public key. The key renewal process is easily accomplished by using the timer in key numbers.

3. Problem Formalization and System Model

Our proposed model is an IoT-based reliable authentication approach to provide the authentication and permission of a soldier by using a mobile device. The authentication is conducted at the fog node/NA and the GH. Each soldier acts as a smart node denoted by $(N) = \{N1, N2, N3 \ldots Nn\}$, where n is the total number of soldiers in the network. In our system model, the soldier sends an encrypted message to the GH to join the group. The GH authenticates the received soldier information by comparing the received values with the actual stored information received from the NA. Moreover, when a soldier is transferred from the present group to another group, the request message is forwarded to the GH. On receiving the request, the GH cooperates with a member node and transfers security credentials to the destination group GHs. Then, the soldier sends the group joining request to the new group. The GH of that group matches the security credentials of the soldier with the pre-received information of the soldier. The GH sends approval to the soldiers and permits soldiers to join the group when the security credentials are matched. Otherwise, the GH cannot join this group. Moreover, NA locally stored and processed the security credentials of the soldiers. The information of soldiers is not available, as the fog node request message is forwarded to the private cloud server for the information of a specific soldier. The information of all soldiers is in the permanent storage of a private cloud server. Security is a necessary element of our proposed scheme to protect the network from several security threats. The authentication process of most existing schemes that use image hashing techniques enhances the communication and computational cost while processing the image. As a solution to this, we provide a secure and lightweight image hashing model. In the case an attacker kills a soldier and takes his mobile device to join the group, the attacker cannot join the group until their security credentials are matched with the security credentials of the soldier that are stored in the private cloud server. In our proposed communication model, Ns, GHs, and NA are the main devices. We utilized asymmetric key-based encryption for secure communication. Moreover, each soldier can only communicate with his GH in the network. The GH can communicate with other GHs in the network and with the NA.

4. Proposed Image Hashing-Based Authentication Scheme

In this section, we present an image hashing-based authentication scheme (IHA). Security is a vital requirement for authentication-based IoT applications. Our scheme provides a solution for secure communication and authentication schemes for emergencies in war. The proposed scheme is subdivided into three phases, namely, node registration, node joining in a group, and the migration of nodes in a group, as shown in Figure 2.

In the registration phase, a soldier is registered at the time of his recruitment. The NA takes the image and other credentials of the soldier stored in the local repositories and further uploads them to the private cloud server for permanent storage. Furthermore, the NA embeds this info (e.g., id, login id, password, and image hash) into the mobile device of the soldier. There will be separate mobile allocations to each soldier. In a war scenario, several soldiers leave and join the groups based on the emergency scenario. In this context, effective authentication and communication are required.

Therefore, the proposed scheme employs a fog node that locally processes the information at the edge of the network. Fog nodes act as a NA that manages the information on the count of groups in the specific network. Moreover, the node count is also considered within these groups. NA forwards the request message for the joining of a soldier in a specific group or the migration of the soldier to a specific group in war situations. A list of notations for the proposed scheme is shown in Table 1.

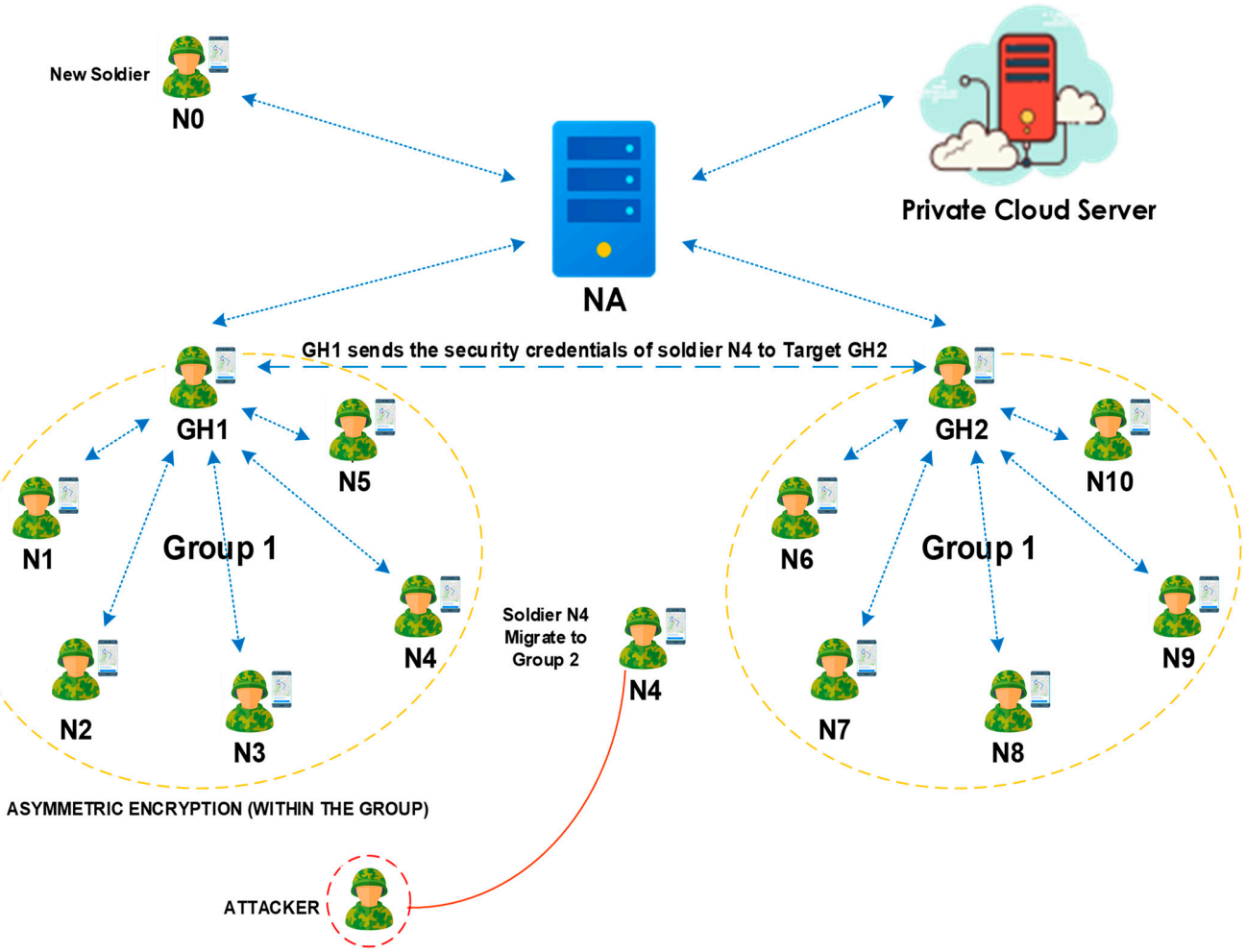


Figure 2. Mobility of node from one group to the other in a secure manner.

Table 1. List of notations for the proposed approach.

Symbol	Description
ID_{Ni}	Node ID
T	Timestamp
RN	Nonce value
H	Hash function
TS	Time stamp
GH_i, GH_j	Group heads in the network
$K_{G_{Hi}}$, $K_{G_{Hj}}$	Public keys of GH_i and GH_j
NA	Network administrator
K_{NA}	Public key of NA
M_{Ni}	Concatenated message of node security credentials
EM_{GH_i}, EM_{Ni}	Encrypted message of node GH_i and node Ni
$H(M_{Ni})$, $H(M_{GH_i})$	Image and security credential hash of node Ni and node GH_i
K_{N_A}, $K_{G_{Hi}}$	Public key of node Ni and node GH_i

4.1. Node Joining Algorithm

In this scenario, the node joining mechanism is explored where the node (Ni) joins a specific group, GH_i. First of all, Ni transmits the join request to GH_i in the form of an encrypted message, as shown in Equations (1) and (2).

$$M_{Ni} = (login\_ID_{Ni} \,||\, pwd_{Ni} ||\, IMG_{Ni}) \quad (1)$$

$$EM_{Ni} = K_{G_H} \{ID_{Ni},\ T_{Ni},\ RN_{Ni},\ H(M_{Ni})\} \quad (2)$$

The message M_{Ni} comprises the login ID ($login\_ID_{Ni}$), the password (pwd_{Ni}), and a hash of the soldier image IMG_{Ni}. The soldier acts as a node and is represented as Ni. Moreover, EM_{Ni} includes the node ID (ID_{Ni}), timestamp (T_{Ni}), nonce value (RN_{Ni}), and a hash of (M_{Ni}) encrypted with the public key ($K_{G_{Hi}}$) of the GH_i. After receiving the join request, the GH_i checks the timestamp of the received message ($T_{Ni} - T_{GH_i}$) < Δt. If the timestamp is greater than the threshold value, then the message is discarded and a request to resend the join request is sent. Otherwise, the GH_i transmits the request message $\{ID_{GH_i},\ T_{GH_i},\ RN_{GH_i},\ Req\ (ID_{Ni})\}$ to the NA by its public key, K_{N_A}, for encryption. Then, the NA forwards the required information based on the ID_{Ni}, as shown in Equations (3) and (4).

$$M_{NA} = (login\_ID_{NA} \,||\, pwd_{NA} ||\, IMG_{NA}) \quad (3)$$

$$EM_{NA} = K_{G_H} \{ID_{NA},\ T_{NA},\ RN_{NA},\ H(M_{NA})\} \quad (4)$$

When a message is received from the NA, GH_i checks the difference of time stamps ($T_{NA} - T_{GH_i}$) < Δt of the received message. In the case of an outdated message, the received message is discarded, and the resend request is shared with the NA. Otherwise, the GH_i authenticates the Ni by comparing the hashes $H(M_{Ni})$ and equals $H(M_{NA})$ received from the Ni and NA. In the case where both the hashes are matched, GH_i adds the Ni to the list of group members. Moreover, the GH_i stores the Ni's information in the group table. Otherwise, the join request is failed as the user is not legitimate or an attacker. The feasible verified steps are shown in Algorithm 1.

Algorithm 1. Node Joining Algorithm

1. $Ni \rightarrow$ **G_{Hi}:** $EM_{Ni} = K_{G_{Hi}} \{ID_{Ni},\ T_{Ni},\ RN_{Ni},\ H(M_{Ni})\}$
2. **G_{Hi}: If** ($T_{Ni} - T_{GH_i}$) < Δt **then**
3. $\quad$ **G_{Hi}** $\rightarrow$ NA**:** $EM_{GHi} = K_{N_A} \{ID_{GH_i},\ T_{GH_i},\ RN_{GH_i},\ Req\ (ID_{Ni})\}$
4. $\quad$ $NA \rightarrow$ **G_{Hi}:** $EM_{NA} = K_{G_{Hi}} \{ID_{NA},\ T_{NA},\ RN_{NA},\ H(M_{NA})\}$
5. $\quad$ **G_{Hi}: If** ($T_{NA} - T_{GH_i}$) < Δt **then**
6. $\quad\quad$ **G_{Hi}: If** $H(M_{Ni})$ equals $H(M_{NA})$ **then**
7. $\quad\quad\quad$ Add Ni in the group and store Ni data
8. $\quad\quad\quad$ Forward success message to Ni and NA
9. $\quad\quad$ **Else**
10. $\quad\quad\quad$ Join request failed
11. $\quad\quad$ **End if**
12. $\quad$ **Else**
13. $\quad\quad$ Drop message and forward resent request of required data
14. $\quad$ **End if**
15. **Else**
16. $\quad$ Discard message and send acknowledgment to Ni for resending join request
17. **End if**

4.2. Node Migration Algorithm

In the case of node migration, a request message is sent to GH_i. After receiving a request from the Ni, the GH_i informs node members. Next, the GH_i transfers security credentials to destination group GH_j. The node migration mechanism is explored in a stepwise manner in Algorithm 2.

Algorithm 2. Node Migration

1. $\boldsymbol{Ni \rightarrow GH_i}$**:** Send migration request $EM_{Ni} = K_{G_{Hi}} \{ID_{Ni},\ RN_{Ni},\ M_{req}\}$
2. $\boldsymbol{GH_i \rightarrow Ni}$**:** Send reply message $EM_{GHi} = K_{N_i} \left\{ID_{Ni},\ RN_{GH},\ K_{G_{Hj}}\right\}$
3. $\boldsymbol{GH_i \rightarrow GH_j}$**:** Send data of Ni to GH_j as $EM_{GH_i} = K_{G_{Hj}} \{ID_{GH_i},\ T_{GH_i},\ RN_{GH_i},\ H(M_{GH_i})\}$
4. $\boldsymbol{GH_j}$: **If** $(T_{GH_i} - T_{GH_j}) < \Delta$t **then**
5. $\quad$ $\boldsymbol{GH_i}$**:** Receive join request from Ni as $EM_{Ni} = K_{G_{Hj}} \{ID_{Ni},\ T_{Ni},\ RN_{Ni},\ H(M_{Ni})\}$
6. $\quad$ **If** $(T_{N_i} - T_{GH_j}) < \Delta$t **then**
7. $\quad\quad$ **If** $H(M_{Ni})$ equals $H(M_{GH_i})$ **then**
8. $\quad\quad\quad$ Add Ni in the group and store Ni data
9. $\quad\quad\quad$ Forward success message to Ni and GH_i
10. $\quad\quad$ **Else**
11. $\quad\quad\quad$ Migration request and join request failed
12. $\quad\quad$ **End if**
13. $\quad$ **Else**
14. $\quad\quad$ Discard the join request of node Ni
15. $\quad$ **End if**
16. **Else**
17. $\quad$ Discard migration request and transmit resend request to GH_i
18. **End if**

In this scenario, the node Ni leaves the current group GH_i to migrate to the remote group GH_j. First of all, Ni forwards the migration request message to the current GH_i. The request message $\{ID_{Ni},\ RN_{Ni},\ M_{req}\}$ is encrypted using the public key $K_{G_{Hi}}$ of GH_i. Then, the GH_i forwards the message $\left\{ID_{Ni},\ RN_{GH},\ K_{G_{Hj}}\right\}$ by encrypting with K_{N_i} as a public key of the Ni. This reply message also includes the $K_{G_{Hj}}$ as a public key of the remote GH_j, as Ni will forward the security credentials to the GH_j for authentication at the time of joining. Moreover, GH_i also forwards the encrypted message, $EM_{GH_i} = K_{G_{Hj}} \{ID_{GH_i},\ T_{GH_i},\ RN_{GH_i},\ H(M_{GH_i})\}$, to the GH_j for authentication purposes. After receiving the security credentials, the GH_j verifies the differences in timestamps as $T_{GH_i} - T_{GH_j}$, which should be less than the threshold time Δt. If the timestamp is greater than the threshold value, then the migration request is discarded, and the resend request is transmitted to the GH_i. Otherwise, the GH_j will receive the message, $\{ID_{Ni},\ T_{Ni},\ RN_{Ni},\ H(M_{Ni})\}$, from the Ni, encrypted using $K_{G_{Hj}}$, to join the new group when the Ni reaches the remote group.

GH_j verifies that the differences in time stamps $(T_{N_i} - T_{GH_j})$ are lower than the threshold Δt. In the case of an outdated message, the received message is discarded. Otherwise, GH_j further compares the hashes $H(M_{Ni})$ and $H(M_{NA})$ for the verification of message integrity. When both the hashes are matched, GH_i accepts the migration and join request of the Ni and stores its information in the group table. Otherwise, the migration and join requests fail, and this node is considered as an unauthenticated node or attacker. The scenario of intergroup migration is shown in Figure 3.

The proposed scheme is evaluated for providing security against the reply attack by including the timestamp and recording the differences between timestamps at the receiving side. This scheme ensures the challenge response from the nodes to ensure authentication and provides secure access control. It involves the hash of values to ensure message integrity against bit-alteration attacks. The image hashing ensures the efficient comparison among the images to reduce computational costs. The proposed scheme ensures that the intruder cannot forge the security parameters taken from the intermediary node traveling from one group to another due to a join or migration operation.

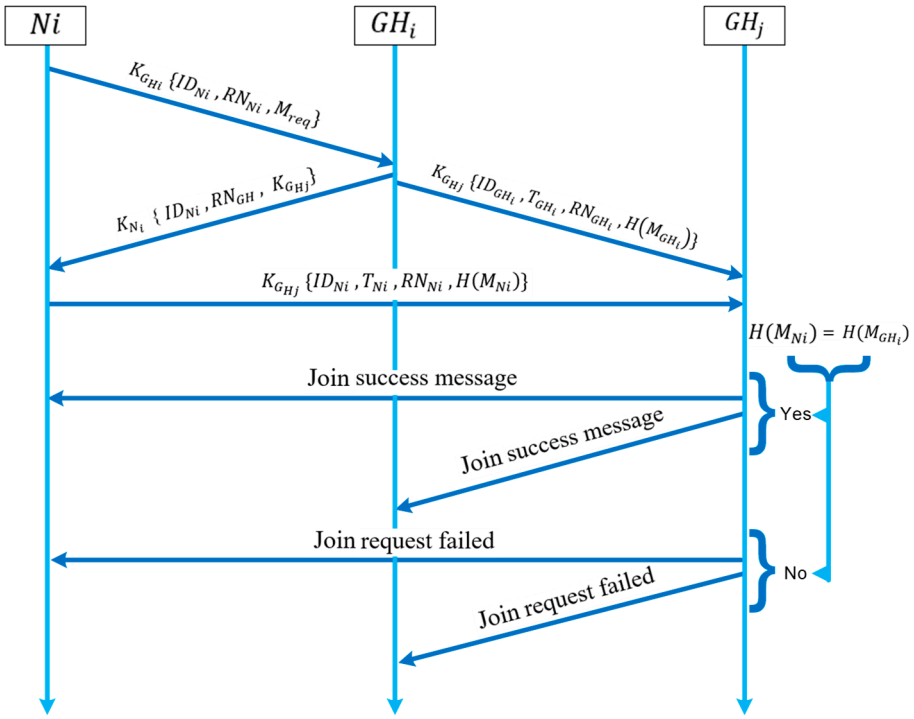


Figure 3. Scenario of intergroup node migrations.

5. Results and Analysis for Performance Evaluation

The proposed work was verified through extensive simulation where nodes were deployed at 1200 m × 1200 m. A simulation was conducted using simulation tool NS 2.35 on Fedora Core 20. In this scenario, TCL was used to create nodes and deploy the network, and for message initiation at particular timeslots. The results were extracted using AWK scripts applied to the trace files. The C language was used for implementing the send, receive, hash, image hash, and security functions. We created separate classes for different levels of devices, such as the GH and NA member nodes. A list of simulation parameters is shown in Table 2.

Table 2. List of simulation parameters.

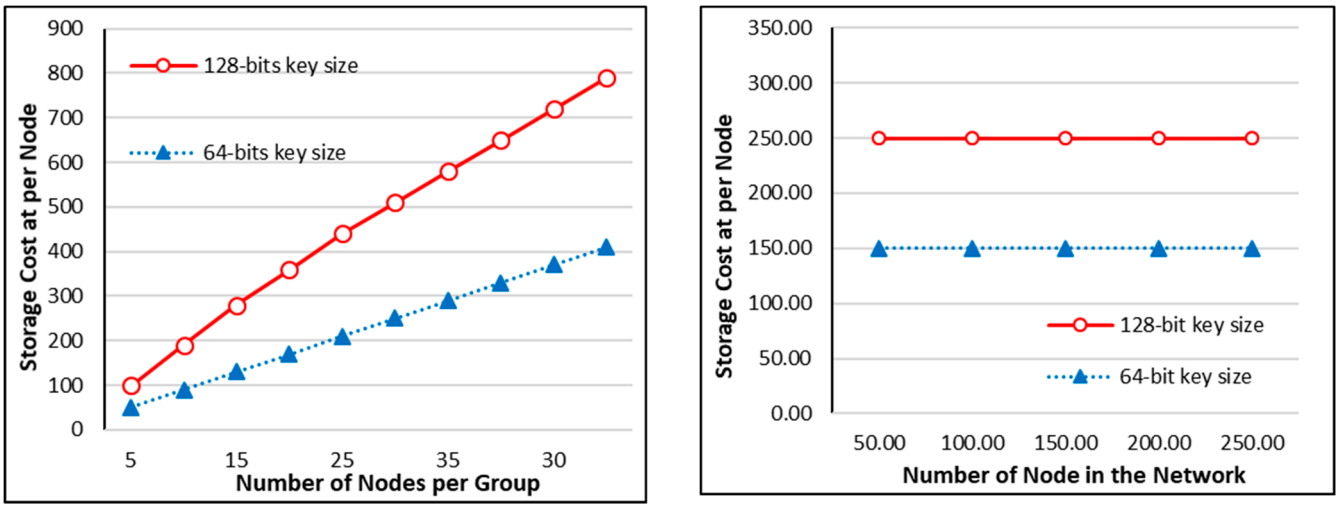
Parameters	Values
Network Area	1200 m × 1200 m
Group Range	400 m
Sensing Range	120 m
Primary Energy of Node	1000 J
Relaying Power	0.819 µJ
Receiving Power	0.049 µJ
Channel Type	Wireless
Communication Framework	Two Ray
Relaying Power of node	0.5819 µJ
Receiving Power	0.049 µJ
Maximum Queue Packets	50
Router Trace	ON
Mac Trace	OFF
Agent Trace	ON
Number of Nodes in a Group	5–30 nodes
Original Data Size	50–400 bytes
Total Number of Message	8–40 messages
Set Time Period	0.1–1.0 s
Number of Nodes	50–250 nodes

In the modeling message, node 0 is a GH at group 1 that forwards the group migration requests of node 4 to the target GH at group 2. Node 6 is a GH at the target group. The message display has a receiving function in node 6 of the target GH, and the message depends on the TCL modeling script sending function. Figure 3 represents the complete setup. However, if the password and image of the node are unverified, then that node will not be permitted from the targeted GH. For example, the source GH (node 0) request for the *Ni* (node 4) is received at the target GH (node 6). The denied responses for joining node 4 are replied to by the target GH (node 6). In this setup, node 4 was unverified, as the hash image and password were not similar to endangered standards.

In this section, the proposed Scheme IHA was examined based on security and efficiency. We compared the proposed IHA scheme with two recent schemes, namely, SRIH [27] and ESIH [28], to prove the supremacy of our proposed scheme. We analyzed our scheme in terms of communication cost, computational cost, memory overhead, failure cost for cluster authentication, and reliability against malicious nodes.

5.1. Memory Overhead

The node of each member holds its public key g-1 and a private key, which is a group size g. For a 64-bit key, if a group consists of 15 soldiers, then each device will have $15 \times 8 = 120$ stored bytes for public keys of 14 soldiers, as well as their private keys. Likewise, when a key has 128 bits, then each device holds 240 bytes. Its group size effect on the requirements for the maintenance of individual nodes is shown in Figure 4a. The results show that increasing the number of bands also enhances the requirement of memory for a device.



(**a**) (**b**)

Figure 4. Storage cost per node in a group is presented in (**a**), whereas the storage cost for the network is presented in (**b**).

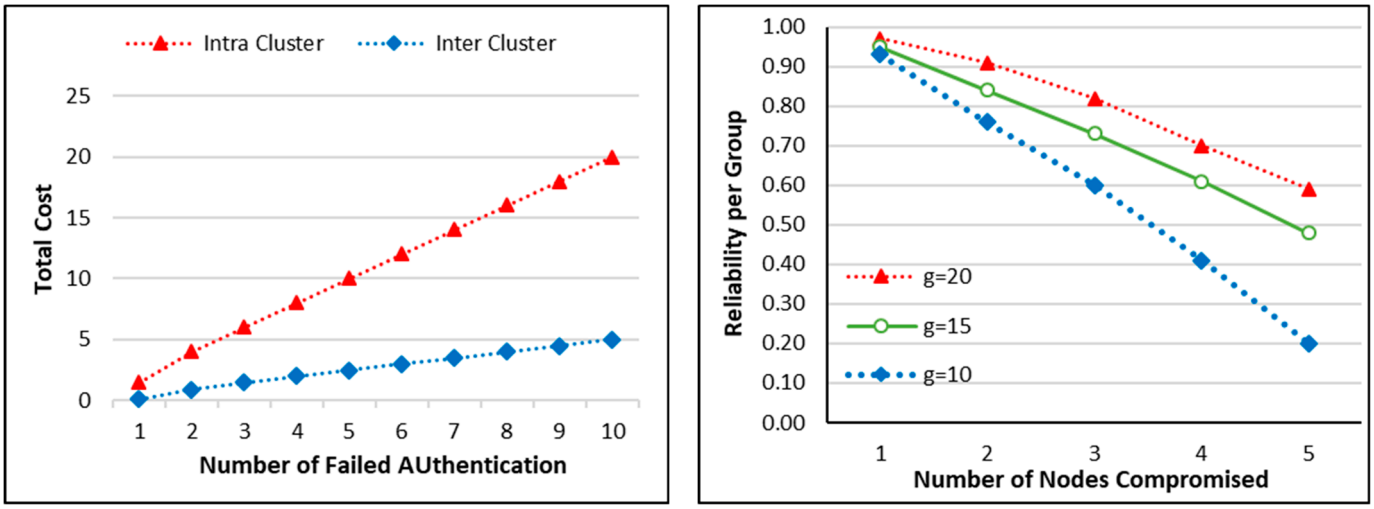
For a key with a 64-bits size, if a group consists of 20 soldiers, then every soldier has $8 \times 20 = 160$ store bytes for 19 public keys and a private key. If the network size increases and the bandwidth remains the same, the storage requirement on a single node will remain the same. Figure 4b illustrates where the size of the network fluctuates from 200 to 2,000 soldiers with a constant number of 20 soldiers. The 128-bit key size results are also presented, where every soldier has $20 \times 16 = 320$ stored bytes, the public keys of 19 soldiers, and their private keys.

5.2. Failure Authentication Cost and Reliability

During the migration process of a node, four internal clusters and two or more cluster messages are shared. The total cost of internal clusters for the process of authentication is wasted when a soldier is attacked before joining. Computational and communication

efforts can be lost in this scenario. During the process of joining, before GH_i testing, four messages will be shared among GH_i, Ni, and NA.

The overall failure authentication cost can be considered as *Total Cost* = *Hfail* × *Mfail*, where *Hfail* is an authentication failure, and *Mfail* represents the amount of failed authentication. The default value *Hfail* is calculated as in Equation (5), where *Lc* and *Kci* are messages to be accounted for, and *Sm* and *Vmi* demonstrate the ability to transmit a message during and between cluster interactions. We observed that during the migration of a node, four cluster messages are transferred within the network, so the value is 4 × 0.1 mJ = 0.4 mJ, as shown in Figure 5a.



(**a**) (**b**)

Figure 5. Cost of failure is shown in (**a**), and the reliability per group is presented in (**b**).

Therefore, if in four groups of 20 nodes, four authentication attempts fail, the total value of the above formula is 1.6 mJ.

$$H_{fail} = (L_c \times S_m) + (K_{ci} \times V_{mi}) \quad (5)$$

Thus, the cost of sending cluster messages is shown separately in Figure 5b, which is estimated to be unsuccessful by an increase in failed authentication. Malicious nodes have an impact on the message transmission reliability of the nodes. When two nodes have a loss of 20 nodes in a group, the reliability of our group is 0.9. This means that our system provides 90% reliability when two combined messages are lost due to two malicious nodes. In this process, 18 nodes can be joined to the group.

5.3. Computational Cost

In the authentication scenario, the *Ni* forwards the security credentials to the GH in the request message to join the specific group. Moreover, the image hashing technique is utilized for node authentication. As shown in Figure 6a, we computed the computational cost in terms of the number of nodes at the GH. The results show that the computational cost varies with the number of nodes. We consider the communication cost when the number of nodes is 200. Then, the computational cost of the IHA, ESIH, and SRIH is 36.79 ms, 98.23 ms, and 104.51 ms, respectively. As shown in Figure 6b, we computed the computational cost in terms of the number of nodes at the NA.

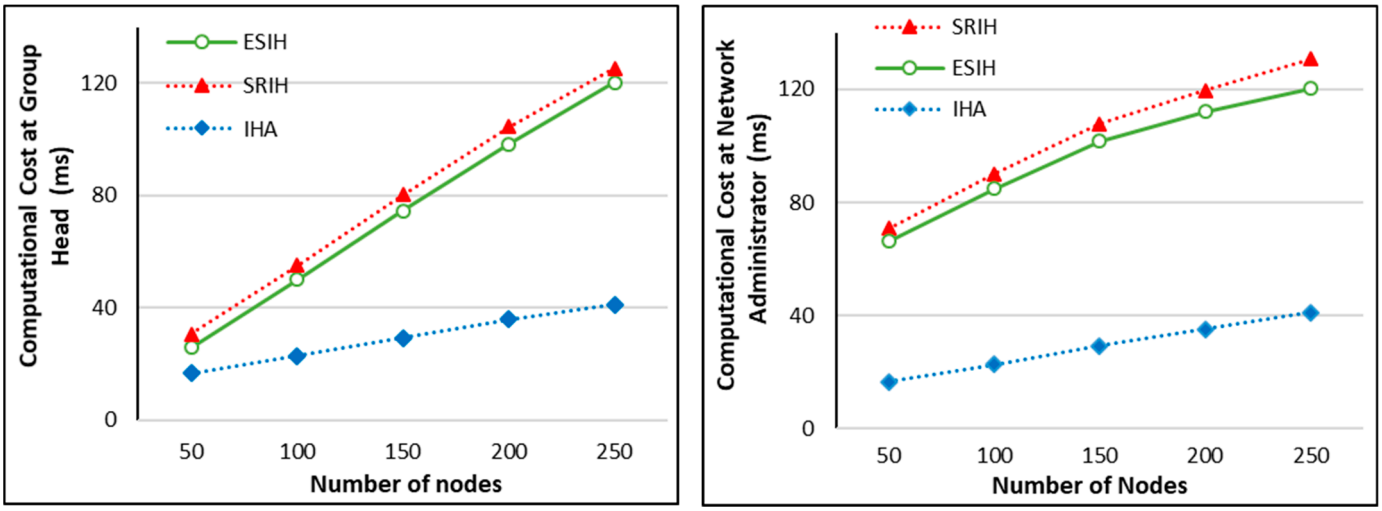
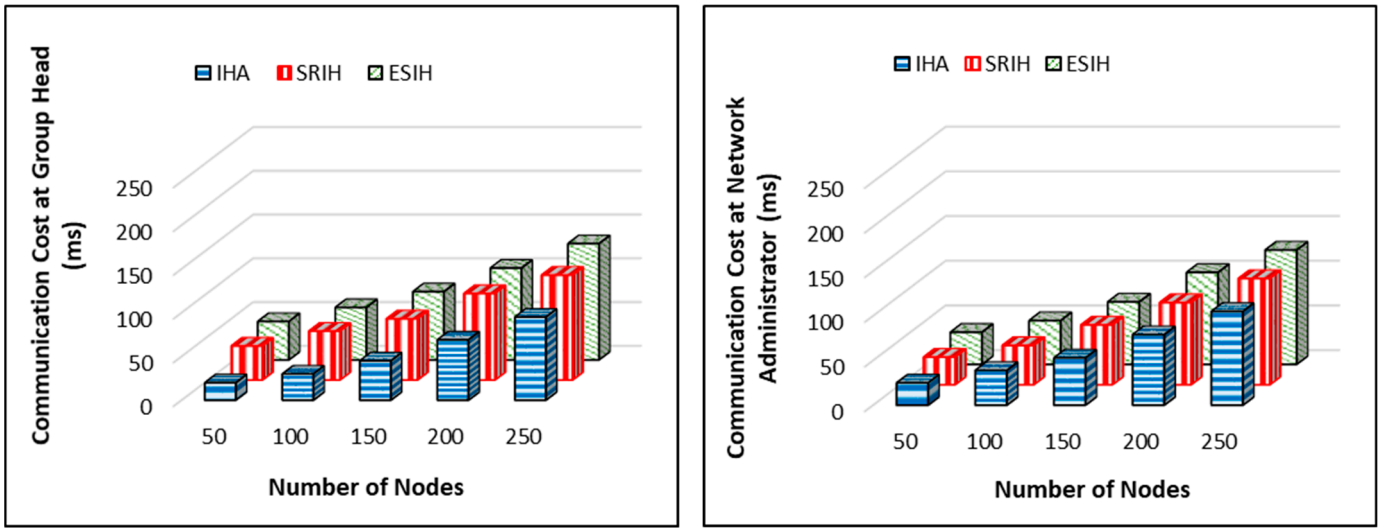


Figure 6. Computational cost is shown for (**a**) group head (GH) and (**b**) network administrator/fog node (NA).

The results show that the computational cost varies with the number of nodes. We consider the communication cost when the number of nodes is 200. Then, the computational cost of the IHA, ESIH, and SRIH is 33.29 ms, 112.04 ms, and 119.61 ms, respectively. The results show that the computational cost of our proposed scheme is lower than that for the SRIH and ESIH, as these schemes also consider the image processing along with image hashing in the node authentication phases. The network administrator forwards the encrypted message with the required security credentials to the GH as per the request. The authentication of the node depends upon the information of the NA.

5.4. Communication Cost

We compared our scheme with SRIH and ESIH schemes to calculate the communication cost with the number of nodes. The registration phase of all the nodes is already established when these nodes join the network. Therefore, the proposed IHA remains efficient with the increase in the number of nodes. The authentication phase is further divided into two phases, communication between GH_i and Ni and communication between GH_i and NA. Figure 7a elaborates the communication cost for phase 1 authentication. In phase 1, for a better understanding, we considered the communication cost for a single node authorization. Thus, Ni forwards the join request to GH_i. In this request, Ni forwards the ID of 16 bits, 64 bits of timestamp, 64 bits of the nonce value, and 256 bits of the hash message. In this case, 400 bits are forwarded to GH_i. The proposed IHA was compared with SRIH and ESIH for the communication cost of authentication phase 1 in terms of the number of nodes. Figure 7b elaborates the communication cost for phase 2 authentication. In phase 2, for a better understanding, we considered the communication cost for a single node. Thus, GH_i forwards the request message of 256 bits to the NA. In reply, the NA forwards the required information message of 400 bits. The proposed IHA was compared with SRIH and ESIH for the communication cost of authentication phase 1 in terms of the number of nodes. The total communication cost was analyzed in both cases based on the total number of nodes. The results show that the communication cost of our proposed scheme is lower than that of the SRIH and ESIH, as these schemes also consider the image processing along with image hashing in the node authentication phases.



(**a**) (**b**)

Figure 7. Communication cost for (**a**) group head and (**b**) network administrator.

6. Conclusions

Mobile ad hoc networks (MANETs) have an essential role to play in future smart environments involving the Internet of Things (IoT) for managing node mobility. In IoT-based systems, they provide self-formation and self-connectedness of networks. Since any node can freely join or leave the network in MANETS, it renders the networks and applications vulnerable to security attacks. Therefore, the provision of secure communication is an essential requirement for nodes in MANETs.

This paper presents a node joining and node migration algorithm for war situations. It involves effective authentication using an image hashing-based security approach which involves a timestamp to guard against a replay attack. The scheme protects against the intruder's attack during the mobility of the node to join the target group. To allow joining, the GH receives the security credentials and hash of images from the node and verifies them with the credentials received from the NA. This reduces the infiltration of vulnerable nodes in the group for war situations or troop-based operations. Moreover, the age of the message is also crosschecked to guard against bit alteration attacks. The proposed work was validated through extensive simulations using NS 2.35. Results elucidate that the proposed scheme dominates its counterparts in terms of computational cost and communication cost for the GH and NA. Moreover, the failure cost of cluster authentication and reliability of malicious nodes is also presented. Results prove the supremacy of our proposed scheme. For the authentication of a node within a group, IHA provides 33% and 30% lower computational costs than SRIH and ESIH, respectively. Moreover, IHA provides 22% and 17% lower communication costs than ESIH and SRIH, respectively.

In the future, we plan to manage two-group fusion and security credential handling under one elected GH with more member nodes.

Funding: This research received no external funding.

Data Availability Statement: Not Applicable, the study does not report any data.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Jan, M.A.; Khan, F.; Alam, M. *Recent Trends and Advances in Wireless and IoT-Enabled Networks*; Springer: Berlin/Heidelberg, Germany, 2019.
2. Du, L.; Ho, A.T.S.; Cong, R. Perceptual hashing for image authentication: A survey. *Signal Process. Image Commun.* **2020**, *81*, 1–63. [CrossRef]

3. Leite, J.R.E.; Martins, P.S.; Ursini, E.L. A Validation Method for AdHoc Network Simulation Including MANETs, VANETs and Emergency Scenarios. In *International Conference on Ad hoc Networks and Wireless*; Springer: Cham, Switzerland, 2019; pp. 32–47.
4. Tambawal, A.B.; Noor, R.M.; Salleh, R.; Chembe, C.; Anisi, M.H.; Michael, O.; Lloret, J. Time division multiple access scheduling strategies for emerging vehicular ad hoc network medium access control protocols: A survey. *Telecommun. Syst.* **2019**, *70*, 595–616. [CrossRef]
5. Aftab, F.; Zhang, Z. Hybrid Self-Organization based Cluster Management Scheme for Group Mobility Aware MANET. In Proceedings of the 2019 28th Wireless and Optical Communications Conference (WOCC), Beijing, China, 9–10 May 2019; pp. 1–6.
6. Noura, M.; Atiquzzaman, M.; Gaedke, M. Interoperability in Internet of Things: Taxonomies and Open Challenges. *Mob. Networks Appl.* **2019**, *24*, 796–809. [CrossRef]
7. Ali, S.; Ahmed, A.; Raza, M. Towards Better Routing Protocols for IoT. In Proceedings of the 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, Pakistan, 30–31 January 2019; pp. 1–5.
8. Singh, V.; Singh, D.; Hassan, M.M. Survey: Black Hole Attack Detection in MANET. In Proceedings of the 2nd International Conference on Advanced Computing and Software Engineering (ICACSE), Sultanpur, India, 8–9 February 2019.
9. Alam, T.; Benaida, M. The Role of Cloud-MANET Framework in the Internet of Things (IoT). *arXiv* **2018**, arXiv:1902.09744. [CrossRef]
10. Sajjad, M.; Haq, I.U.; Lloret, J.; Ding, W.; Muhammad, K. Robust Image Hashing Based Efficient Authentication for Smart Industrial Environment. *IEEE Trans. Ind. Inform.* **2019**, *15*, 6541–6550. [CrossRef]
11. Du, L.; He, Z.; Wang, Y.; Wang, X.; Ho, A.T.S. An Image Hashing Algorithm for Authentication with Multi-Attack Reference Generation and Adaptive Thresholding. *Algorithms* **2020**, *13*, 227. [CrossRef]
12. Alnumay, W.; Ghosh, U.; Chatterjee, P. A Trust-Based Predictive Model for Mobile Ad Hoc Network in Internet of Things. *Sensors* **2019**, *19*, 1467. [CrossRef] [PubMed]
13. Desai, A.M.; Jhaveri, R.H. Secure routing in mobile Ad hoc networks: A predictive approach. *Int. J. Inf. Technol.* **2019**, *11*, 345–356. [CrossRef]
14. Rath, M.; Panigrahi, C.R. Prioritization of Security Measures at the Junction of MANET and IoT. In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies, Udaipur, India, 4–5 March 2016; p. 127.
15. Belgaum, M.R.; Musa, S.; Su'ud, M.M.; Alam, M.; Soomro, S.; Alansari, Z. Secured Approach Towards Reactive Routing Protocols Using Triple Factor in Mobile Adhoc Networks. *arXiv* **2019**, arXiv:1904.01826.
16. Dhanya, K.; Jeyalakshmi, C.; Balakumar, A. A Secure Autonomic Mobile Ad hoc Network based Trusted Routing Proposal. In Proceedings of the 2019 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 23–25 January 2019; pp. 1–6.
17. Khan, F.; Rehman, A.U.; Yahya, A.; Jan, M.A.; Chuma, J.; Tan, Z.; Hussain, K. A Quality of Service-Aware Secured Communication Scheme for Internet of Things-Based Networks. *Sensors* **2019**, *19*, 4321. [CrossRef] [PubMed]
18. Zhao, H.-Y.; Wang, J.-C.; Guan, X.; Wang, Z.; He, Y.-H.; Xie, H.-L. Ant Colony Based Energy Consumption Optimization for Mobile IoT Networks. In Proceedings of the 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Atlanta, GA, USA, 14–17 July 2019; pp. 118–122.
19. Saleem, M.A.; Shijie, Z.; Sharif, A. Data Transmission Using IoT in Vehicular Ad-Hoc Networks in Smart City Congestion. *Mob. Networks Appl.* **2019**, *24*, 248–258. [CrossRef]
20. Stulman, A.; Stulman, A. Secured by Fluctuating Topology Using the Fluctuating Topology of MANETs to Secure Key Exchange. *Electronics* **2019**, *8*, 1172. [CrossRef]
21. Zhang, D.-G.; Gao, J.-X.; Liu, X.-H.; Zhang, T.; Zhao, D.-X. Novel approach of distributed & adaptive trust metrics for MANET. *Wirel. Networks* **2019**, *25*, 3587–3603. [CrossRef]
22. Khan, B.U.I.; Olanrewaju, R.F.; Anwar, F.; Mir, R.N. ECM-GT: Design of Efficient Computational Modelling based on Game Theoretical Approach Towards Enhancing the Security Solutions in MANET. *Int. J. Innov. Technol. Explor. Eng.* **2019**, *8*, 506–519.
23. Olanrewaju, R.F.; Khan, B.U.I.; Anwar, F.; Mir, R.N.; Yaacob, M.; Mehraj, T. Bayesian Signaling Game Based Efficient Security Model for MANETs. In Proceedings of the Future of Information and Communication Conference, San Francisco, CA, USA, 14–15 March 2019; pp. 1106–1122.
24. Mohammad, S.N.; Singh, R.P.; Dey, A.; Ahmad, S.J. ESMBCRT: Enhance Security to MANETs Against Black Hole Attack Using MCR Technique. In *Innovations in Electronics and Communication Engineering*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 319–326.
25. Van Vinh, N.; Kim, M.-K.; Jun, H.; Tung, N.Q. Group-based public-key management for self-securing large mobile ad hoc networks. In Proceedings of the 2007 International Forum on Strategic Technology (IFOST), Ulaanbaatar, Mongolia, 3–6 October 2007.
26. Pushpa Lakshmi, R.; Kumar, A.A. Cluster Based Composite Key Management in Mobile Ad Hoc Networks. *Int. J. Comput. Appl.* **2010**, *4*, 36–42. [CrossRef]
27. Bashir, I.; Ahmed, F.; Ahmad, J.; Boulila, W.; Alharbi, N. A Secure and Robust Image Hashing Scheme Using Gaussian Pyramids. *Entropy* **2019**, *21*, 1132. [CrossRef]
28. Chen, H.; Huang, X.; Wei, W.; Yi, M. Efficient and secure image authentication with robustness and versatility. *Inf. Sci.* **2020**, *63*, 1–18. [CrossRef]