MPR Based Secure Content Routing Scheme for NDN-MANET

Xian Guo, Ma-Jiang Zhang, Aristide Ngaboyindekwe, Jun-Li Fang, Jing Wang

School of Computer and Communication, Lanzhou University of Technology, China
{iamxg, zmajiang}@163.com, bonheur235@yahoo.fr, {fangjl, wangjing}@lut.cn

Abstract

"Bread Crumb" routing in native NDN is better suitable for highly dynamic MANET. However, uncontrolled interest flooding will cause the broadcast storm and security issues in NDN-MANET. So, this paper takes advantage of MPR in OLSR and proposes a MPR based Secure Content Routing for NDN-MANET (MPR-SCR). In this novel scheme, some security mechanisms, such as cooperative authentication, statistical detection, and voting scheme etc., are introduced to resolve security issues mentioned in this paper. By using cooperative authentication based on Merkle Tree, nodes in a network can cooperatively verify a new node that wants to join the network. PIT based statistical detection, that benefits from NDN's stateful forwarding feature, and voting scheme are used to prevent from selecting a node that is controlled by an attacker, as a node in MPR. And they can further block attacks of interest flooding and sending malicious name prefix. In addition, hash and signature mechanisms in an interest packet are used for source authentication. Finally, we simply analyze security attributes of our novel scheme, and detailly verify our scheme and make comparisons with the related schemes by experiment in ndnSIM 2.3.

Keywords: Named data networking, MANET, Merkle tree, Secure content routing

1 Introduction

Information-Centric Networking (ICN) architecture is attracting extensive attentions [1-3] since "Networking Named Content" was proposed in [4]. Researchers in academic and industrial areas are exploring mechanisms that integrate ICN in MANET [1], IoT [2], VANET [3] etc.. NDN (Named Data Networking) [5] is one of the most important instances of ICN and research on content routing is an essential problem in NDN.

In [1], routing solutions used in ICN-MANET were comprehensively elaborated. The authors summarize the existing content routings for ICN-MANET from different dimensions. It is similar with MANET routing based on IP that content routing can be classified into two main classes: proactive (e.g., MobileCCN [6] and TOP-CCN [7]), and reactive (e.g., E-CHANET [8] and REMIF [9]). MobileCCN is a routing based on Internet routing RIP [10] and TOP-CCN is a routing based on MANET routing OLSR [11]. These two protocols E-CHANET and REMIF are the extensions of AODV [12] so that they can be used in ICN-MANET.

These ICN-based schemes for MANET routing have pros and cons [13]. The proactive routing can be used to create FIB in response to an up-to-date network topology but has some overheads of routing control message exchange. Contrarily, the reactive routing has no overheads of routing but has some overheads of Interest packet transfer. These two routing classes can be applied in different environments. A hybrid routing protocol for ICN-MANET is proposed in [13]. This new routing combines mechanism in proactive and reactive routing.

In addition, these existing routings for ICN-MANET mainly focus on how to achieve ICN in MANET, routing performance and security issues are not considered. In ICN, packet flooding in a routing update will produce large quantity copies, which will cause PIT and FIB table overload. PIT and FIB are two important components for content routing. In [14], the authors analyze security issues in ICN and concluded that: (1) when the requested content does not exist or need to be dynamically generated, then the PIT overload caused by interest flooding will lead to DoS/DDoS attacks, which will seriously affect the response time of the user to access the data. (2) By hijacking the routing node and tampering an interest packet for the routing update, the attacker can release the bogus routing announcement, which will lead to the error of the FIB table and destroy the consistency of the routing information recorded by nodes in the network. (3) In native ICN, no security mechanism is used in an interest packet, so that the attacker can tamper and forge the interest packet. These security problems also exist in ICN-MANET.

In order to resolve the above security problems in ICN routing, an interest traceback mechanism is proposed in [15]. This mechanism can mitigate DoS attack by tracing the originator of the malicious packet. However, the problem (e.g., flooding) triggered by the

*Corresponding Author: Xian Guo; E-mail: iamxg@163.com
DOI: 10.3966/160792642019092005026

interest packet itself was not considered in [15]. In [16], a solution of rate limiting for each end user was proposed. Because the concept of host ID (e.g., IP address) is not used in ICN, the attacker can easily issue a content request exceeding this limit. So, it is difficult to completely solve the problem by using this mechanism [16]. An Interest Negative Acknowledgement (NACK) solution is proposed in [17]. The mechanism can alleviate the interest flooding to a certain degree. However, the network will be filled with NACK replications, which will aggravate the network congestion, when the attacker requests a large number of non-existent content. In [18], the cooperative filtering mechanism among routing nodes has been proposed. In this solution, a fuzzy logic set is constructed by using the statistical information of PIT table in ICN. Once the malicious prefix in an interest packet that may be issued by an attacker was detected on a routing node, the interface that the interest packet enters will be limited. Although the mechanism can effectively detect the malicious prefix that the attacker issued, the speed limiting on an interface can degrade the overall performance of the routing. In [19], a proactive interest flooding detection and mitigation mechanism called route tokens which proactively provide NDN a quantifiable degree of security against interest flooding without relying on a stateful forwarding plane is proposed. However, the congestion caused by interest flooding was not resolved in this scheme.

"Bread Crumb" routing is used in native NDN. That is to say, a content consumer firstly initiates an interest packet. And then an intermediate node in a network will remember the upstream node that forwards an interest packet and continues to broadcast the received interest packet. When a content provider receives an interest packet that requests content, it will generate and forward the content packet to the interface that the first interest packet entered. The node on the bread crumb routing will forward the content packet and remember the name prefix of content in FIB. This mechanism is a reactive routing scheme and better suitable for highly dynamical MANET. However, uncontrolled packet flooding that used in the scheme can cause the broadcast storm in the wireless communication environment. MPR (Multiple Point Relay) scheme used in OLSR (a popular protocol in MANET) [11] can efficiently resolve this problem (such as broadcast storm and collision) caused by flooding. This paper proposes a MPR based Secure Content Routing (MPR-SCR) solution for NDN-MANET. In this novel scheme, MPR is used to reduce the number of redundant packets in interest flooding. This paper considers link cost, nodes connectivity, and some special parameters (for example, the PIT occupancy ratio used in this paper) to set up a MPR set that can represent the truest state of a network. In addition, security mechanisms such as Merkle Tree [20], voting scheme [21] and PIT based statistical detection are introduced to solve the interest flooding, DoS attack and attack caused by malicious prefix request and tampering an interest packet. At the same time, these mechanisms can reduce the probability that a compromised node enters MPR. To ensure the integrity, source authentication of an interest packet, hash and signature mechanisms are used in MPR-SCR. Finally, we simply analyze security attributes in an informal method and verify correctness, feasibility and reliability of new solution in ndnSIM 2.3.

The remainder of this paper is organized as follows: Section 2 introduces preliminaries. Section 3 describes the system model used in this paper. Section 4 describes details of our proposed scheme. Section 5 simply analyzes security attributes of our scheme, Section 6 presents evaluation results and finally Section 7 concludes our paper.

2 Preliminaries

2.1 NDN Communication Model

NDN is a consumer-driven communication model. Its communication process is shown in Figure 1. The content consumer generally uses an interest packet to request the interested content by content name. Intermediate nodes that have received an interest packet will firstly choose one or more interfaces from their outgoing faces, and then forward the interest packet to the next hop node. Eventually, the content owner, that can be the content producer or some in-network nodes who forwarded the requested content will reply with a data packet. Note that the data packet is self-certification. That is to say, the data packet will carry data-integrity and authentication information according to receiving an interest packet. So, this feature enables in-network caching. In native NDN, the network node will route the data packet back to the consumer according to the "bread crumb" routing left by the interest at the intermediate nodes. Three basic components are required to implement the above communication process. These three components are respectively PIT (Pending Interest Table), FIB (Forwarding Information Base) and CS (Content Store). Here, the PIT table is used to record the pending interest packets. So, a corresponding "pending interest" entry will be added to the PIT table when an intermediate node has forwarded an interest packet through some of its outgoing faces. The FIB table is used to store name prefixes (domains) and their corresponding outgoing face. In NDN, CS is a content repository to store the content forwarded by the network node.

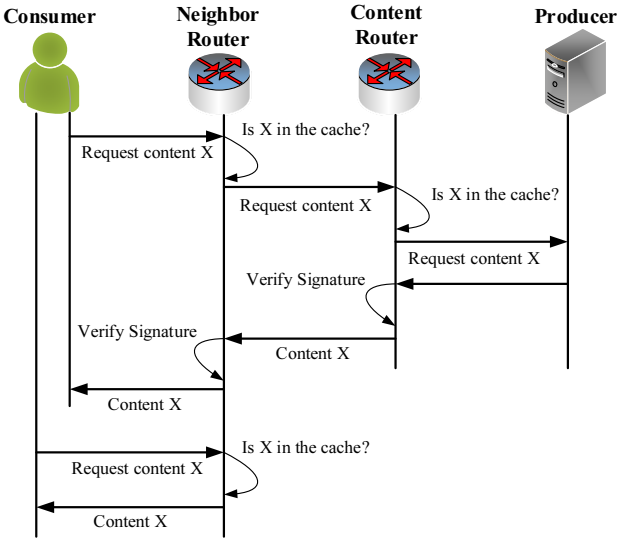

Figure 1. NDN communication model

In NDN communication model, the stateful feature of routing benefits from the routing component PIT table, reflects that a node has forwarded an interest packet used to request some content, but it has not yet received a reply for this request. PIT table records the content request information which includes a content name CN, a Nonce got from the corresponding interest packet, Interface ID for the received interest packet, Interface ID that is used to forward the interest packet to the next-hop and the Sending-time: the time that the interest packet is forwarded to the next-hop. In addition, a Timer is used for each entry in the PIT table to determine whether each entry is satisfied or expired by comparing the sending time. The incoming interface information allows data to be returned along the reverse path of the request, reflecting the symmetric routing in NDN.

2.2 OLSR

Optimized Link-State Routing (OLSR) [11], specially designed to satisfy the requirements of MANET is an optimization of the classical link state algorithm LSR used in IP network. The key concept used in this protocol is that of multipoint relays (MPRs) used to forward routing control information whereby a set of partial neighboring nodes selected according to some strategy. The goal of a node in a process that sets up its MPR set is to allow as little 1-hop nodes as possible in a MPR set to forward the packets to many 2-hop nodes as possible that connected to it, namely, the most 2-hop nodes that can be reached through a minimum number of 1-hop nodes. That is to say, a node will forward a received message to some nodes in MPRs rather than in all of the neighboring nodes. So, this mechanism can efficiently reduce the message overload caused by flooding.

In OLSR, there are two types of routing control packets: Hello packet and TC (Topology Control) packet. Hello packet is used to establish a node's neighbor list and calculate its MPR; TC packet is used to calculate the topology of the network. The routing process of OLSR is described as follows: a node periodically broadcasts Hello message to its neighbors, and uses an MPR selection algorithm (described in OLSR [11]) to calculate its own MPR set according to the information returned by the neighbor nodes. Then, the node broadcasts the TC packet to the whole network through the MPR nodes, and the other nodes calculate the routing table after receiving the TC packets.

2.3 Merkle Tree

Merkle Tree (MT) [20], also known as the hash tree, was proposed by the computer scientist Ralph Merkle in 1972. It is a data structure which has the following features: each leaf node of a tree is composed of a hash of the data, the hash values of all the sub-nodes under each parent node are combined and then subjected to a hash operation to get their parent nodes. The process continues till the hash operation gets the root of the tree. For example, in Figure 2, the process of generating the parent node $Node_9$ from the leaf nodes $Node_1$ and $Node_2$ can be expressed by the following equation (1):

$$Node_9 = H\left(H\left(Node_1\right) \| H\left(Node_2\right)\right) \quad \textbf{(1)}$$

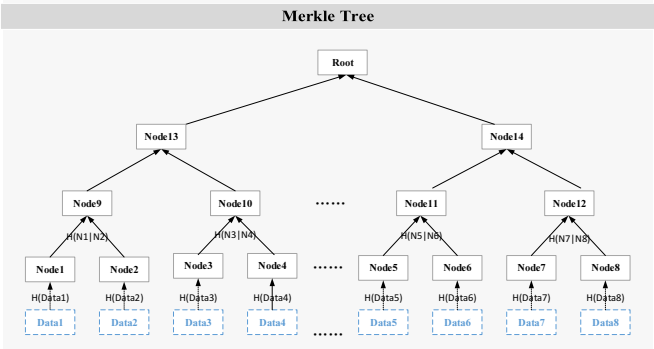

Figure 2. The structure of MT

It is one of the main advantages of MT that it can independently provide integrity authentication for all leaf nodes on the tree by simply performing a signature operation on the root node once.

MT that is a full binary tree is usually used for digital signature [18] in which multiple hash functions are used to generate a public key. Being obtained through a particular authentication path, the key of each leaf node can be compared with the public key to achieve certification. The authentication path is made up of a node on each layer of the tree, which last from the sibling node of the leaf path to the next layer of the root node. As shown in Figure 2, the full authentication path for data Data1 in MT is: $\{Node_2, Node_{10}, Node_{14}\}$.

2.4 Byzantine General Agreement

The Byzantine General issue, also known as the *t*-elasticity agreement, is a fundamental problem in the point-to-point communication proposed by Lamport [21] in 1978. Its primary meaning is that how many loyalty generals can make a correct and consistent decision in the presence of a traitor. The *t*-elasticity agreement is an algorithm such that, on the one hand, there are some traitors who could make trouble but cannot be found, and on the other hand, the *t*-elasticity agreement also needs to make sure the loyal generals can reach a consensus.

Lamport proved that there was no *t*-elasticity agreement under 3*t* generals, but there must be a *t*-elasticity agreement under 3*t*+1 generals or above. That means, to tolerate the presence of a traitor and also get a consistent decision, that agreement must ensure the total number of generals is greater than 3*t*.

3 System Model

3.1 Network Model

To illustrate our secure routing scheme MPR-SCR, the simplified network model for NDN-MANET is shown in Figure 3; this paper mainly focuses on the routing of the network part *N* in NDN-MANET. It is assumed that the number of the nodes is n_N in the network *N* (where the nodes have the dual roles of router and device). n_i (i=1, 2, …, *N*) are used to mark a node. Here, the node *P* is the content producer who is abstracted from n_i, and the node *C* is a user who is interested in some content in the network, namely, content consumer. It is assumed that there only exists one node in the network *N* at initialization. When a new node wants to join the network, it firstly registers to TTP (Trusted Third Party, this TTP can be online or offline) and gets some cryptographic materials needed in the subsequent communication process. And then the new node will send the authentication information received from cryptographic materials to other nodes in the network so that the nodes in the network can cooperatively verify the identity of a new node by using a scheme based on Merkle Tree. The corresponding cryptographic materials will be revoked after a node has left the network. In the network *N*, the process that an honest node forwards an interest or data packet still follows the communication mechanism in native NDN.

3.2 Threaten Model

This paper mainly focuses on the problems caused by interest flooding. It is assumed that all nodes in the network will strictly follow the rule of the native NDN in the process of forwarding data packet. So, this paper mainly discusses security problems in these two phases: network initialization and forwarding an interest packet.

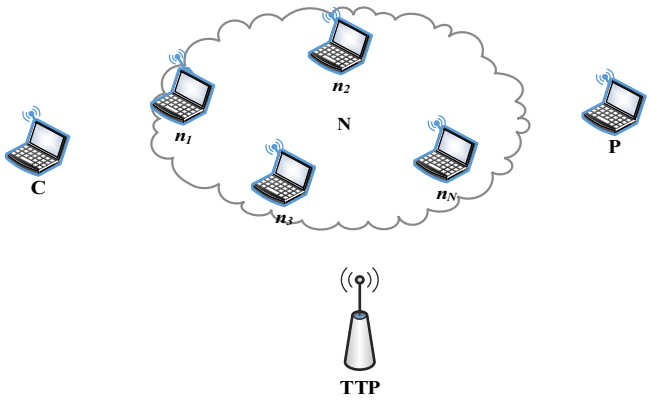

Figure 3. Simplified NDN-MANET network model

Both active attack and passive attack are considered in these two phases.

Network initialization phase. In this stage, the possible attack scenarios are that an attacker can intercept and tamper the authentication information that a new node sends to the network so that an honest node can't join the network. The attacker can also capture and control a new node that wants to join the network, consequently fake the honest node to join the network.

ForwarDing an interest packet phase. In native NDN, no cryptographic mechanism in an interest packet is used for efficiency consideration. So, an attacker can easily tamper a received interest packet, which will cause interest flooding and DoS attacks. The attacker can also send a large number of invalid content requests that request non-existence content in the network, which will result in a PIT table filled with some invalid requests, so that the legal request of honest user can't get a correct response before a timer for an interest packet expires.

In addition, a selectively forwarding attack is also an attack that is easily achieved. An upstream node controlled by an attacker may partially forward or discard a received interest packet. Consequently a downstream node will fail to receive the content packet, so that the downstream node's PIT table is filled with some expired interest items.

4 MPR-SCR Scheme

The new solution MPR-SCR uses the mechanism of bread crumb routing in native NDN to transmit data instead of using any routing protocol. However, uncontrolled interest flooding can cause the broadcast storm in wireless broadcast communication and can also increase the probability that an attacker performs an attack on a network. So, this paper takes advantage of MPR in OLSR in our novel scheme. In addition, to prevent these attacks mentioned in section 3.2, some security mechanisms are introduced. Firstly, in order to achieve cooperative authentication to a new node that wants to join the network, an authentication scheme

based on Merkle tree is proposed in MPR-SCR. Secondly, the MPR-SCR makes use of NDN's stateful forwarding feature described in section 2.1, a PIT based statistical detection scheme is proposed in our MPR-SCR. Combining this detection scheme with voting scheme can prevent from selecting a node controlled by an attacker as a node in MPR. Furthermore, hash and signature mechanisms are introduced to achieve message integrity authentication and source authentication in an interest packet.

4.1 Network Initialization

In our scheme MPR-SCR, it is assumed that a network can contain the maximum number of nodes is n_N. TTP will set up a Merkle Tree *MT* with n_N key chains. It will select a key chain from *MT* and distribute the selected key chain to a new node that requests to join into a network, and TTP will also distribute a final value k_0 of this key chain to other nodes in the network. The steps that TTP creates a Merkle Tree *MT* are described as follows.

Step 1: TTP Constructs a Key Chain that Will be Used on *MT*

TTP randomly selects a seed S_r from a sufficiently large Galois field *GF(p):* {1, 2, ..., *p-1*} (*p* is the order of Galois field, and *p* must be a large prime number), and then iteratively calculates *n* times for the seed S_r by using a one-way hash function (e.g., SHA-1) to generate a key chain $k_c = \{k_0, k_1, ..., k_{n-1}\}$ required in MPR-SCR scheme. The iterative calculation of this k_c is shown as follows:

$$\begin{cases} k_{n-1} = H(S_r) \\ k_{n-2} = H(k_{n-1}) \\ \cdots \\ k_1 = H(k_2) \\ k_0 = H(k_1) \end{cases} \quad (2)$$

For any $0 \le i \le n-1$, the i^{th} iterative calculation of the one-way hash for the key chain can be expressed as: $k_i = H(k_{i+1})$, where *H* is a one-way hash function, k_0 is a final value of this key chain and will be sent to other nodes in the network.

Step 2: TTP Creates a Merkle Tree *MT*

According to the Byzantine General Issue described in section 2.4, each node in the network needs at least *m* ($m \ge 3t+1$, where *t* is the number of malicious nodes that may exist in the network) piece of information to allow other nodes to verify its identity. Therefore, an algorithm *Creation_Merkle_Tree*() that sets up a Merkle Tree *MT* is described in Table 1.

Table 1. Merkle tree set up algorithm

***Creation_Merkle_Tree*(n_N, *m*)**

```
Begin
  For i from 1 to n_N:
    creates the i^th key chain
    randomly selects a seed S_ri
    For j from 1 to m:
      uses the seed S_ri to generate a hash key chain
      k_cj according to equation (2).
    Endfor
  Endfor
End
```

According to these one-way key chains generated in the algorithm *Creation_Merkle_Tree*(), the Merkle Tree *MT* constructed by TTP is shown in Figure 4.

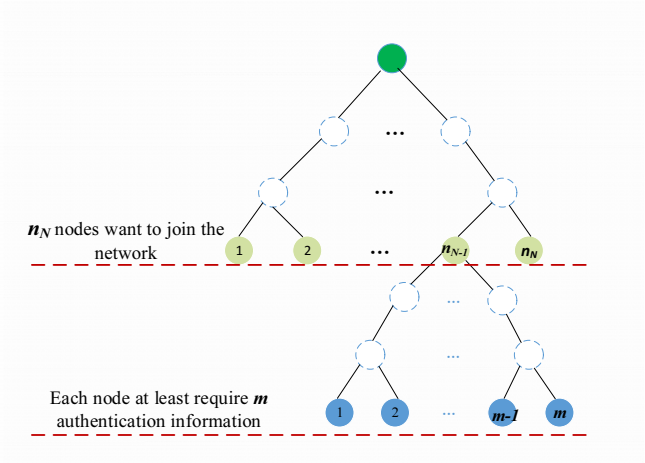

Figure 4. Merkle tree *MT* created by TTP

4.2 Joining a Network

Step 1: TTP Distributes Cryptographic Materials

To join a network, a new node *A* will firstly register to TTP in a secure channel. The node *A* will obtain *m* pieces of authentication information $\{k_1 \| k_2 \| \cdots \| k_m\}$ from the Merkle Tree *MT*. At the same time, TTP distributes the corresponding path $\{path_{k_1} \| path_{k_2} \| \cdots \| path_{k_m} \| k_0\}$ of the *m* pieces of authentication information and the corresponding final value k_0 to nodes on the network. In addition, TTP will generate and save public certification of a new node according to a public key that the new node provided.

Step 2: Nodes in the Network Cooperatively Verify the Identity of a New Node

A new node will firstly provide its authentication information $\{k_1 \| k_2 \| \cdots \| k_m\}$ that received from TTP to other nodes in the network. Other nodes in the network perform verification operations on these authentication information. If the new node can't offer enough information generated on *MT* in a certain period or if

other nodes can't validate these information on *MT* according to the corresponding path information and final value k_0 $\{ path_{k_1} \| path_{k_2} \| \cdots \| path_{k_m} \| k_0 \}$, then it will be rejected and will be added to a blacklist of other nodes.

After successfully running the above two steps and the new node isn't added to a blacklist of any one node, the new node will become a node in NDN-MANET.

4.3 Setting up a MPR Set

In our MPR-SCR mechanism, in order to reduce redundant packets caused by interest flooding, a node in the network will only forward a received interest packet to nodes in a MPR set instead of broadcasting the received interest packet to all of the neighboring nodes as in the native NDN. However, an attacker may forge adjacent information to add a node controlled by an attacker to MPR of another node. To prevent this attack, the paper introduces a voting scheme and a statistical detection scheme based on PIT table.

4.3.1 PIT Based Statistical Detection

In order to achieve a statistical detection mechanism based on PIT table described in section 2.1, two terms are firstly defined: PIT Occupancy Rate (*POR*) and PIT Expiration Rate (*PER*).

$$POR = \frac{R_{cur}}{C_{max}},\ PER = \frac{E_{cur}}{R_{cur}} \quad \textbf{(3)}$$

Where R_{cur} is number of current records in PIT, E_{cur} is number of records that just expire and C_{max} is a max capacity of PIT. *POR* reflects a consumption degree of the PIT table resource. *PER* reflects a degree that content requests of consumers are satisfied. And *PER* also indirectly reflects the network congestion degree. Experimental observation indicates that *POR* and *PER* values will abnormally increase when an attack (e.g., interest flooding) occurs in the network. The statistical detection based on PIT is described as follows:

Step 1. Each node in the network periodically detects and calculates the *POR* and *PER* values according to its PIT table by using equation (3).

Step 2. When one of *POR* and *PER* or both are greater than the preset threshold in a node, the node will immediately generate an interest packet with a special flag *flag*. The format of the interest packet is similar to equation (5) described in section 4.4. The node will forward this flagged packet to the downstream node. The packet is considered as a warning message and contains the name prefixes information $MPLT_m$ that is recorded in the corresponding PIT entry. This name prefix may incur the above *POR* and *PER* value to become abnormally large. In addition, the reason that sends the flagged packet to a downstream node is that the node in upstream can aggregate more traffics than a downstream node according to the prefix aggregation in native NDN, and a downstream node is closer to the location of the attacker.

After receiving the above warning message, the downstream nodes will record the malicious prefix information $MPLT_m$ and broadcast it to its neighbor nodes. The node that detects the malicious prefix will vote 1 for the node that forwarded the malicious prefix, according to the voting scheme described in section 4.3.2.

4.3.2 Voting Scheme

In MPR-SCR, nodes in a network will record behaviors of its adjacent nodes and will vote to other nodes. If a node detects a malicious behavior of a node, it will vote the node 1. Otherwise, it will vote 0. For example, a node receives a large number of interest packets from some node or detects a malicious prefix according to the scheme described in section 4.3.1; it will vote the node 1. All nodes in the network will periodically exchange their voting values on other nodes and respectively count these voting results. If the number of nodes that vote 1 on some node reaches a certain threshold, then it means that the node is a compromised node and will be added to a blacklist BLT_m of other nodes.

4.3.3 MPR Selection Algorithm

To set up a MPR set, a node will firstly calculate MPR_{cost} of its every neighboring node (Of course, except for nodes in a blacklist generated according to voting scheme described in section 4.3.2) by using the following equation (4):

$$MPR_{\cos t_i} = (1-\alpha) \times (\frac{n_{1-hop}}{n_{2-hop}})_i + \alpha \times POR_i \quad \textbf{(4)}$$

Where $\alpha \in [0,1]$, i is the node ID of a neighboring node, $(\frac{n_{1-hop}}{n_{2-hop}})_i$ is a ratio between the number of 1-hop neighbors of the node i and that of 2-hop neighbors, and POR_i represents PIT occupancy rate of the node i described in section 4.3.1. Here, the computation of MPR_{cost} considers both a network connectivity and forwarding efficiency, because the $(\frac{n_{1-hop}}{n_{2-hop}})_i$ reflects the number of 1-hop and 2-hop neighboring nodes connected to a node, and the POR_i implicitly reveals the packets forwarding status of a node. The node will select a neighbor node that the $MPR_{\cos t_i}$ value is maximum as a next-hop node and add it to its MPR set in each process till the 2-hop set become an empty set ϕ. For any node A_n who wants to set up its MPR set, the selection algorithm *MPR_selection()* is described in Table 2.

Table 2. MPR selection algorithm

MPR_Selection():

Begin
  $MPR=\emptyset$
  $TMP_i=\emptyset$
  $S_{1\text{-}hop}$ = {nodes: *a 1-hop neighbor set of* A_n}
  $S_{2\text{-}hop}$ = {nodes: *a 2-hop neighbor set of* A_n}
  For i from 1 to num($S_{1\text{-}hop}$):
    If $S_{2\text{-}hop}$! = $\emptyset$:
      uses equation (4) to calculate $MPR_{\cos t_i}$ of each node between A_n and the i^{th} node in $S_{1\text{-}hop}$.
      selects the node n_x with a maximum $MPR_{\cos t_i}$
      MPR=MPR$\cup\{n_x\}$
      TMP_i=$TMP_i\cup$ {nodes: 1-hop neighbors of n_x}
      $S_{2\text{-}hop} = S_{2\text{-}hop} - TMP_i$
    EndIf
  EndFor
End

4.4 Requesting an Interested Content

To request an interested content, a consumer node C will send interest packets to all of the nodes in its MPR set that generated in section 4.3. The format of a composite interest packet is described as follows.

$$\{ID_C \,||\, IntL||\, k_i||\, H(IntL||\, k_i)||SIG_{S_C}(H(IntL||\, k_i))\} \quad \textbf{(5)}$$

Where ID_C is an identifier of the node C, $IntL$ contains all general information such as a requested content name, nonce, etc. that required in an interest packet in native NDN. $H(.)$ is a hash value. $SIG_{S_C}(.)$ is a signature of this consumer on a hash value of *Intl* and k_i. S_C is a private key of this consumer node, and the corresponding public key P_C is managed by TTP.

4.5 Forwarding an Interest Packet

Step 1. When a node receives an interest packet, it firstly performs a source legitimacy authentication of the key k_i in the interest packet as follows:

$$H^i(k_i) = k_0 \quad \textbf{(6)}$$

Where H is a one-way hash function that generated the corresponding key chain, and k_0 is a final value of the key chain that includes k_i.

Step 2. If the verification fails in the step 1, the interest packet will be deleted. And it will vote the interest generator 1. Otherwise, the node that receives the interest packet will request public key certification of the node from TTP and then will verify the signature $SIG_{S_C}(.)$ in the interest packet. If this signature verification fails or there exists content that the consumer requests in its content storage *CS*, then the node will discard the received interest packet. Otherwise, it will forward the interest packet to nodes in its MPR set and modify its NDN components according to the rule of NDN.

4.6 Generating a Data Packet on a Content Producer

When a content producer in the network receives a legal interest packet, which means that the verifications in section 4.5 successful, the node will generate and forward a content packet to the interface that received the first interest packet. The content producer will delete other interest packets that will arrive later. The format of the content packet is described as follows.

$$\{ID_P||SIG_{S_P}(H(ID_P||content))||symenc_{k_{CP}}(ID_P||content)\} \quad \textbf{(7)}$$

Where ID_P is an identifier of the content producer P, $H(.)$ is a hash value. $SIG_{S_P}(.)$ is a signature of the content producer by using its private key on *content* that will be issued and its identifier ID_P, and $symenc_{k_{CP}}(.)$ is ciphertext generated by using a pre-shared key k_{CP} between the content producer P and the consumer node C that sent the interest packet.

4.7 Generating a Data Packet on an Intermediate Node

When a node in the network receives a legal interest packet, which means that the verifications in section 4.5 are successful, the node will check whether there exists a content that matches with the received interest packet in its content storage CS. If the node has no content that a consumer requests in the interest packet, it will forward the received interest packet according to the rule of section 4.4. Otherwise, it will generate and forward a content packet that contains the requested content according to the NDN rule. The format of the content packet is same as equation (7) described in section 4.6.

4.8 Forwarding a Data Packet

When an intermediate node receives a data packet, it firstly does a signature verification of the content provider in the data packet. If this verification fails, it will vote the content provider 1, and delete this data packet. Otherwise, it will save the relative information in its CS according to the rule of NDN.

4.9 Revoking a Key Chain

After a node hears that one of its neighbors is unreachable, it will initiate a voting process for confirming this failure. When other nodes' votes for the unreachable node have reached a revocation threshold, the node that initiates the voting process will declare that the unreachable node has left the network, and it will send a revocation request to the TTP. After receiving a revocation request, the TTP will delete the key chain that assigned to the node that has left the network and update the *MT*.

The transmitted message in our scheme is shown in Table 3.

Table 3. Message transmitted in MPR-SCR

A node *A* joins a network.
$n_A \rightarrow TTP: \{ID_A \parallel P_A \parallel nonce\}$
$TTP \rightarrow n_A: \{k_1 \parallel k_2 \parallel ... \parallel k_m\}$
$TTP \rightarrow N: \{path_{k_1} \parallel path_{k_2} \parallel ... \parallel path_{k_m} \parallel k_0\}$
Some node *X* sends malicious prefixes and blacklist collected in communication process.
$n_X \rightarrow MPR: \begin{Bmatrix} flag \Vert ID_X \parallel IntL \parallel MPLT_m \parallel BLT \parallel k_i \parallel H(IntL \parallel MPLT_m \parallel \\ BLT \Vert k_i) \parallel SIG_{S_X}(H(IntL \parallel MPLT_m \parallel BLT \Vert k_i)) \end{Bmatrix}$
Some consumer node *C* requests an interested content:
$n_C \rightarrow \text{MPR}: \{ID_C \Vert IntL \Vert k_i \Vert H(IntL \Vert k_i) \Vert SIG_{S_C}(H(IntL \Vert k_i))\}$
An intermediate node *I* forwards the received interest packet:
$n_I \rightarrow \text{MPR}: \{ID_C \Vert IntL \Vert k_i \Vert H(IntL \Vert k_i) \Vert SIG_{S_C}(H(IntL \Vert k_i))\}$
A content provider *P* sends a content packet
$n_P \rightarrow n_x: \{ID_P \Vert SIG_{S_P}(ID_P \Vert H(content)) \Vert symenc_{k_{CP}}(ID_P \Vert content)\}$
An intermediate node *I* forwards the received content packet to node in the upstream:
$n_P \rightarrow n_u: \{ID_P \Vert SIG_{S_P}(H(ID_P \Vert content)) \Vert symenc_{k_{CP}}(ID_P \Vert content)\}$

5 Security Analysis

Proposition 1. An outside node can't join a network that uses MPR-SCR.

Proof. (1) A new node that wants to join a network firstly is required to register to TTP. TTP will verify the identity of this node and will issue some cryptographic materials such as k_i on a key chain that will distribute to this node on Merkle Tree *MT*.

(2) In addition, when a new node joins a network, it is required to provide $\{k_1 \parallel k_2 \parallel ... \parallel k_m\}$ got from TTP. And then other nodes perform cooperative authentication on this new node according to information $\{path_{k_1} \parallel path_{k_2} \parallel ... \parallel path_{k_m} \parallel k_0\}$ from TTP.

So, in summary, an outside node won't join the network that uses MPR-SCR.

Proposition 2. Any network node can prove that any received interest packet must come from a declared consumer node and is not tampered in transmission.

Proof. The signature algorithm and Hash() are introduced in an interest packet of our scheme MPR-SCR. A node is firstly required to calculate $H^*(.)$ value according to the received information and k_i. If this new Hash() value $H^*(.)$ is equal to the received value $H(.)$, then the interest packet is not tampered in transmission. And then, the node will verify the signature $SIG_{S_C}(.)$ by using a public key P_C that got from TTP. If this verification is successful, then it can be proven that the received interest packet must come from the declared consumer.

Proposition 3. A consumer node can prove that a received data packet must come from a declared content provider and is not tampered in transmission. It can also be proven that other nodes can't read content in this data packet.

Proof. The consumer node will first verify the signature of the content provider *P* by using a public key P_P that got from TTP. If this verification is successful, then it has been proven that the content packet comes from the declared content provider. And then it will perform decryption operation by using a pre-shared key k_{CP} between the consumer node *C* and the content provider *P*. If it can successfully decrypt this ciphertext $symenc_{k_{CP}}(.)$, then it has further been proven this content packet comes from the content provider *P* and content can't be read or tampered in transmission.

Proposition 4. An intermediate node can prove that a received data packet must come from a declared content provider.

Proof. After receiving the data packet from the other node, the intermediate node firstly requests the public key P_p of the producer *P* from the TTP, and then uses the public key P_p to verify the signature information in the received data packet. If the signature verification is successful, it means that the data packet received by this intermediate node is indeed from the claimed producers.

6 Simulation Analysis

In order to verify the correctness, feasibility and reliability of the MPR-SCR scheme proposed in this paper, the performance and security mechanisms of MPR-SCR are firstly analyzed, and then we make a comparison analysis between MPR-SCR and the most related schemes proposed in [16] and [18]. For simulation, ndnSIM 2.3 simulation tool developed by NDN project team is used. It is assumed that there exist 25 nodes in this NDN-MANET. The simulation topology of NDN-MANET is shown in Figure 5,

where $C_i\left(i=1,2,\cdots,9\right)$ are the content consumer nodes, $R_i\left(i=1,2,\cdots,7\right)$ are the intermediate nodes, and $P_i\left(i=1,2,\cdots,9\right)$ are the content producer nodes. The parameters used in the simulation are listed in Table 4.

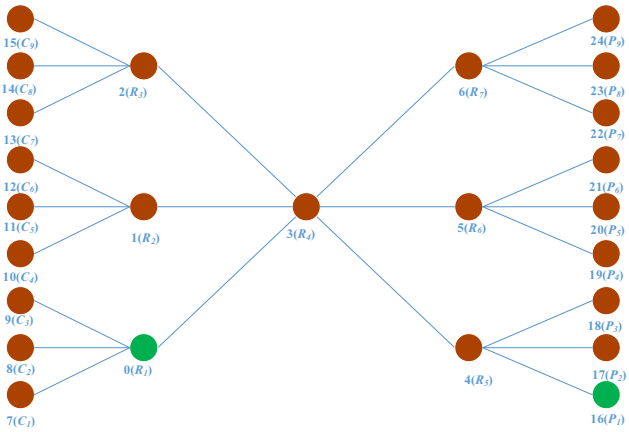

Figure 5. Simulation topology

Table 4. Simulation parameters

Wireless Communication protocol	IEEE 802.11a 20Mb/s
Mobility model	RandomWalked2DMob-ilityModel 1m/s
CS strategy	LRU
CS size	1000 content items
PIT strategy	Persistent
Maximum PIT size	150 entries
Expired time of PIT entry	5s
Size of each content item	1024byte
Forwarding strategy	BestRoute/Multicast
Rate of legitimate Interest	200 Ints/s
Duration for legitimate Interest	0-60s
Rate of malicious user	20 Ints/s
Duration for malicious Interests	20-50s

6.1 Solution Verification

6.1.1 With_MPR vs. Without_MPR

In our MPR-SCR, in order to limit the number of interest packets transmitted on the network, nodes in the network only forward a received interest packet to neighboring nodes in MPR. So, in this simulation, we make a comparison between the bread crumb routing in native NDN and an improved content routing based on MPR to observe the advantage that MPR is adopted.

As seen in this simulation in Figure 6, the number of interest packets transmitted on the network increase with the number of 1-hop neighbors. However, in our MPR-SCR, only nodes in MPR are required to retransmit a received interest packet, which significantly reduces the number of packets as compared to the flooding strategy in original bread crumb routing since MPR is a subset of 1-hop neighbors of a node.

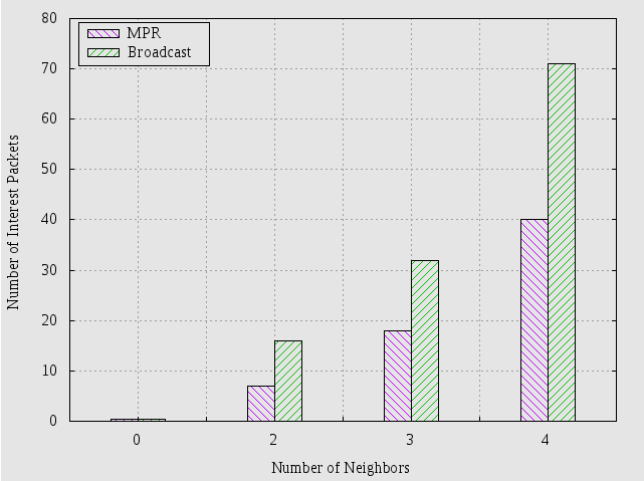

Figure 6. Relationship between number of packets transmitted and number of neighbors

In a wireless environment, congestion and collision caused by the broadcast storm can lead to packets loss, and flooding makes this problem more serious. In MPR-SCR, the usage of MPR degrades channel competition due to the reduction of packet retransmission, resulting in an obviously lower packet loss as shown in Figure 7.

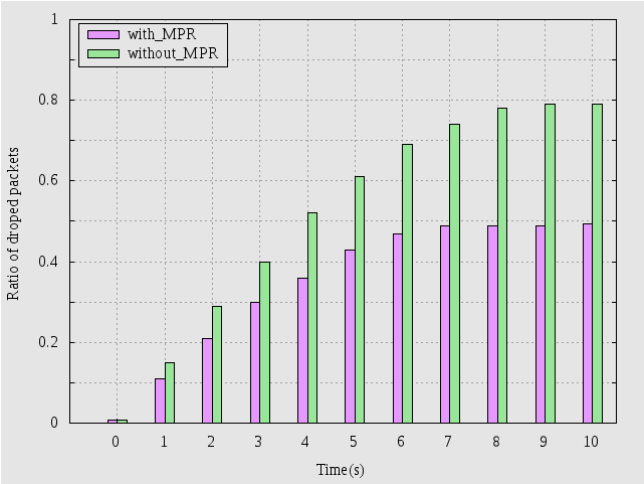

Figure 7. Ratio of dropped packets

6.1.2 Variation on PIT Entries

For security mechanism verification, this experiment selects an intermediate node R_1 as the observation node. In addition, it is assumed that P_1 is a content producer. That means the content requested by the nodes (including normal and malicious requests) in an interest packet eventually will come from the content provider P_1.

In this simulation, this paper firstly analyzes a number variation of PIT entries in the different expiration time of an interest packet. This simulation selects 5 different timeout values for comparison. Clearly, the simulation in Figure 8 indicates that increase of expiration time has a great impact on the number of entries in the PIT table. At the same time, it

can be concluded that the smaller this simulation selects a timeout value, the fewer a node records entry of interest packets in the PIT. Because the larger this simulation selects an expiration time, the longer each interest request will be allowed to wait in PIT table, which will dramatically increase the number of entries in the PIT.

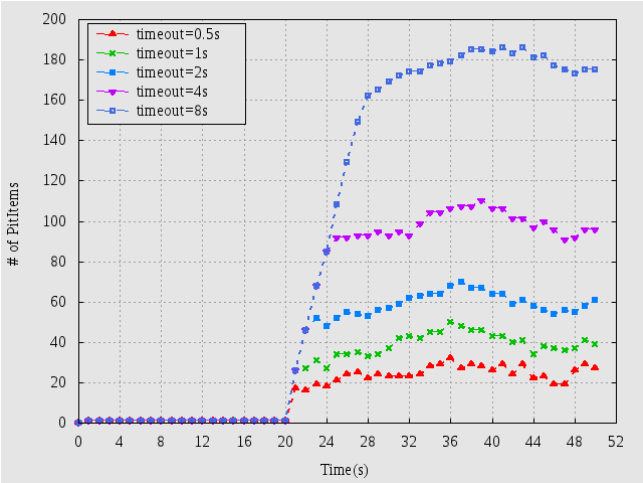

Figure 8. Number of PIT entries under different expiration times

In addition, we compare a variation of the number of entries in the PIT table in these three cases: normal, attack without prevention scheme, and attack with MPT-SCR. In a normal network, the number of PIT entry maintains a constant value of 78 in figure 9. Because the timeout value that this simulation sets is 5s for each interest packet, the corresponding information for each interest packet will be recorded in the PIT table before timeout or this interest packet is satisfied. In attack scenarios that a node sends a malicious request to request non-existence content or send a large number of requests, the number of entries in a PIT table will increase dramatically because no node can satisfy the malicious request and each request information will keep in the PIT until it expires. A malicious request will be discarded when our MPR-SCR scheme is used, thus the PIT table's entries will be decreased.

6.1.3 Variation on *POR* and *PER*

Figure 10 reflects the real-time expiration rate of entries in PIT table under normal circumstances and attack. Normally, an interest packet can always be satisfied before the timeout, and therefore there is no expired entry in the PIT. However, when the network is attacked, no node can satisfy these malicious interest requests. So, each entry will keep in the PIT until they expire, which will result in a more significant *PER* value under the attack.

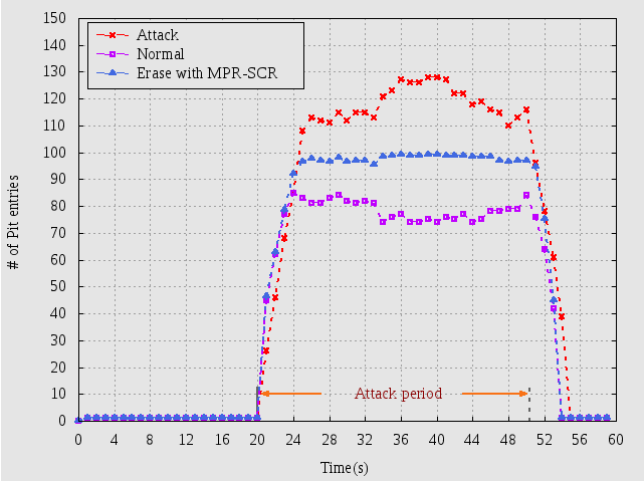

Figure 9. The number of PIT entries in different cases

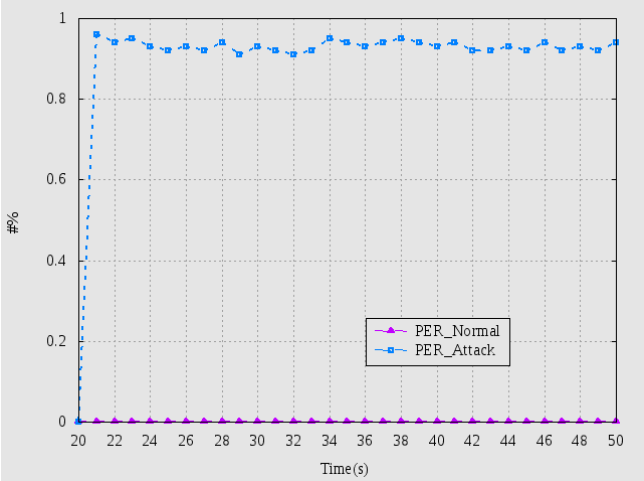

Figure 10. PIT expiration rate

In Figure 11, three curves respectively show a variation of *POR* in the following three cases: normal, attack without prevention scheme, and attack with MPR-SCR. In normal circumstance, namely, there is no malicious node in this network, *POR* will maintain a lower value. When the network is under attack, *POR* will maintain a large value in contrast to the normal case. It is rational because some interest request can't be satisfied. However, although *POR* value will increase sharply at the beginning, then it will gradually decrease and approach to the normal value without attack when MPR-SCR is used. In MPR-SCR, since nodes are required to send a warning message to downstream nodes after detecting an abnormal *POR* value. So, according to receive a warning message, downstream nodes will record the malicious request and broadcast the information to its neighbor nodes, thus preventing further harm of malicious requests.

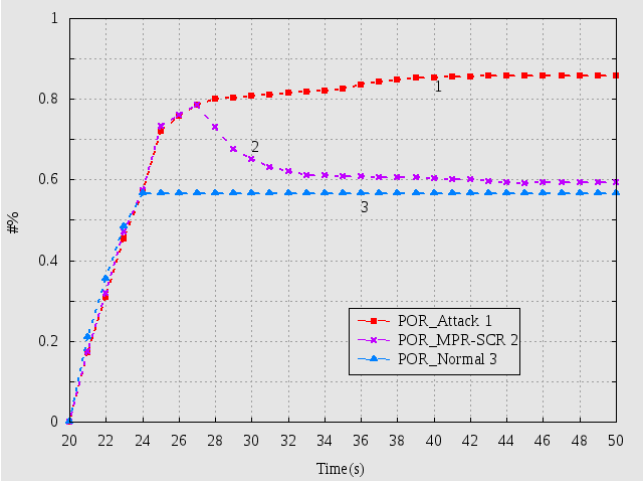

Figure 11. PIT occupancy rate

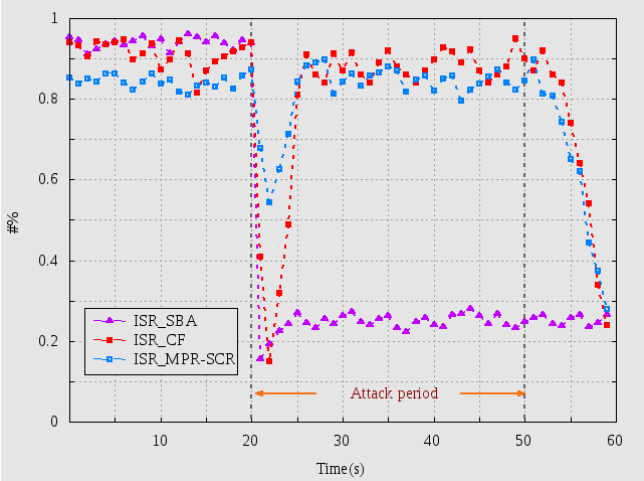

Figure 12. ISR variation under different schemes

6.2 Simulative Comparisons

ISR (Interest Satisfaction Rate) is an important performance index of routing in NDN, this analyzes ISR and make a comparison between our scheme and the most related schemes in the literature [16] and [18]. This paper name the scheme [16] as SBA and the scheme [18] as CF.

It can be seen from Figure12 that, under attack case, the average value of ISR_SBA is around 25%, and that of ISR_CF is 89%. But we also note that ISR_CF will drop to 18% in attack instantaneous, and the recovery is slow. In our MPR-SCR, the average ISR_MPR-SCR value will reach 86% when there exists attack in the network, and the minimum value of ISR_MPR-SCR will also reach 55%, and what's more, the recovery time is shorter than that of CF. It can be concluded that the ISR of SBA is the lowest. Although the CF scheme has a higher ISR, fluctuation also is more significant than that of SBA and MPR-SCR and response also is slower than that of SBA and MPR-SCR under attack. The reason for this difference is that security schemes such as cooperative authentication and PIT based statistical detection and so on, are introduced in MPR-SCR. In particular, voting scheme among nodes can ensure a quick response to a malicious request issued by a compromised node controlled by an attacker.

7 Conclusion

NDN is an important future Internet architecture. Routing is a challenging problem in highly dynamic MANET. Bread crumb routing in native NDN is better suitable for MANET. So, we explore a method that applies NDN in MANET. To resolve broadcast storm in wireless broadcast communication, MPR is introduced in our scheme MPR-SCR. The experiment shows that MPR based interest packet forwarding can significantly decrease the number of interest packet retransmission. To prevent attacks caused by interest flooding or a malicious interest request, some security mechanisms such as cooperative authentication, voting, PIT based statistical detection and so on are proposed in MPR-SCR. The experiment shows these security schemes can efficiently mitigate attack impacts caused by the overload of PIT table due to malicious requests and interest flooding. For example, PIT occupancy rate also can keep a normal level and Interest Satisfaction Rate can reach 86% even if there exist malicious nodes in a network. Our solution can be used for some network environment with high security requirements such as tactical MANET.

Acknowledgements

This work is supported by NSFC No. 61461027, No. 61462060, No. 61562059; Gansu province science and technology plan project under grant No. 1610RJYA 0086; Overseas exchange fund for faculty of the Lanzhou University of Technology. We thank the referees for helpful comments.

References

[1] Xuan Liu, Zhuo Li, Peng Yang, Yongqing Dong, Information-centric Mobile Ad Hoc Networks and Content Routing: A Survey, *Ad Hoc Networks*, Vol. 58, pp. 255-268, April, 2017.

[2] Baccelli E, Mehlis C, Hahm O, Thomas C. S, Information Centric Networking in the IoT: Experiments with NDN in the Wild, *ACM-ICN '14 Proceedings of the 1st ACM Conference on Information-Centric Networking*, Paris, France, 2014, pp. 77-86.

[3] Amadeo M, Campolo C, Molinaro A, Information-centric Networking for Connected Vehicles: A Survey and Future Perspectives, *IEEE Communications Magazine*, Vol. 54, No. 2, pp. 98-104, February, 2016.

[4] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, R. L. Braynard, Networking Named Content, *Communications of the ACM*, Vol. 55, No. 1, pp. 117-124, January, 2012.

[5] D. Saxena, V. Raychoudhury, N. Suri, C. Becker, J. Cao, Named Data Networking: A Survey, *Computer Science Review*, Vol. 19, pp. 15-55, February, 2016.

[6] S. Yao, X. Zhang, F. Lao, Z. Guo, MobileCCN: Wireless Ad-hoc Content-centric Networks over SmartPhone, *Proceedings of the 8th International Conference on Future Internet Technologies*, Beijing, China, 2013, pp. 1-2.

[7] J. Kim, D. Shin, Y. B. Ko, TOP-CCN: Topology Aware Content Centric Networking for Mobile Ad Hoc Networks, *2013 19th IEEE International Conference on Networks*, Singapore, Singapore, 2013, pp. 1-6.

[8] M. Amadeo, A. Molinaro, G. Ruggeri, E-CHANET: Routing, Forwarding and Transport in Information-Centric Multihop Wireless Networks, *Computer Communications*, Vol. 36, No. 7, pp. 792-803, April, 2013.

[9] R. A. Rehman, T. D. Hieu, H. M. Bae, S. H. Mah, B. S. Kim, Robust and Efficient Multipath Interest Forwarding for NDN-based MANETs, *2016 9th IFIP Wireless and Mobile Networking Conference*, Colmar, France, 2016, pp. 187-192.

[10] G. Malkin, RIP Version 2, *IETF RFC 2453*, November, 1998.

[11] T. Clausen, P. Jacquet, Optimized Link State Routing Protocol (OLSR), *IETF RFC 3626*, October, 2003.

[12] C. Perkins, E. Belding-Royer, S. Das, Ad Hoc On-Demand Distance Vector (AODV) Routing, *IETF RFC 3561*, July, 2003.

[13] N. Q. Minh, R. Yamamoto, S. Ohzahata, T. Kato, A Routing Protocol Proposal for NDN Based Ad Hoc Networks Combining Proactive and Reactive Routing Mechanisms, *The Thirteenth Advanced International Conference on Telecommunications*, Venice, Italy, 2017, pp. 78-83.

[14] R. Tourani, S. Misra, T. Mick, G. Panwar, Security, Privacy, and Access Control in Information-Centric Networking: A Survey, *IEEE Communications Surveys & Tutorials*, Vol. 20, No. 1, pp. 566-600, September, 2017.

[15] H. Dai, Y. Wang, J. Fan, B. Liu, Mitigate DDoS Attacks in NDN by interest traceback, *2013 IEEE Conference on Computer Communications Workshops*, Turin, Italy, 2013, pp.381-386.

[16] A. Afanasyev, P. Mahadevan, I. Moiseenko, Interest flooding attack and countermeasures in Named Data Networking, *2013 IFIP Networking Conference*, Brooklyn, USA, 2013, pp. 1-9.

[17] C. Yi, A. Afanasyev, I. Moiseenko, L. Wang, B. C. Zhang, L. X. Zhang, A Case for Stateful Forwarding Plane, *Computer Communications*, Vol. 36, No. 7, pp. 779-791, April, 2013.

[18] K. Wang, H. C. Zhou, Y. C. Qin, H. K. Zhang, Cooperative-Filter: Countering Interest Flooding Attacks in Named Data networking, *Soft Computing*, Vol. 18, No. 9, pp. 1803-1813, September, 2014.

[19] A. Alston, T. Refaei, Neutralizing Interest Flooding Attacks in Named Data Networks Using Cryptographic Route Tokens, *2016 IEEE 15th International Symposium on Network Computing and Applications*, Cambridge, USA, 2016, pp. 85-88.

[20] G. Becker, *Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis*, Ruhr-Universität, 2008.

[21] L. Lamport, Time, Clocks, and the Ordering of Events in a Distributed System, *Communications of the Acm*, Vol. 21, No. 7, pp. 558-565, July, 1978.

Biographies

Xian Guo is currently an Associate Professor of Computer and Communication School of Lanzhou University of Technology. He received PhD and MS in Lanzhou University of Technology, China, in 2008 and 2011, respectively, and BS in Nothwest Normal University. His interest fields are Future Internet Architecture, secure routing in wireless sensor networks and security of Internet of Things and so on.

Ma-Jiang Zhang is currently a Master student at Computer and Communication School of Lanzhou University of Technology. He received his Bachelor degree from Anhui University of Technology in 2014, and started his master studying in 2015. His research interests are Future Internet Architecture, security of wireless network.

Aristide Ngaboyindekwe is currently a Master student at Computer and Communication School of Lanzhou University of Technology. He received his Bachelor degree in Electronics and Communication Systems from National University of Rwanda in 2012 and started his master studying in 2016. His research interests are Future Internet Architecture, security of wireless network.

Jun-Li Fang is a lecturer of Computer and Communication School of Lanzhou University of Technology. She received BS and MS in Beijing Jiaotong University, China, in 2007 and 2009. Her research interests include network and information security.

Jing Wang is currently a lecturer of Computer and Communication School of Lanzhou University of Technology. He is a doctoral candidate,and received BS and MS in Lanzhou University of Technology, China, in 2004 and 2007, His interest fields are security of Industrial control systems and Internet of Things and so on.