Preventing Unauthorized Messages and Achieving End-to-End Security in Delay Tolerant Heterogeneous Wireless Networks

Hany Samuel and Weihua Zhuang
Department of Electrical and Computer Engineering, University of Waterloo, Ontario, Canada
Email: {hsamuel, wzhuang}@bbcr.uwaterloo.ca

***Abstract*—Maintaining user connectivity over heterogeneous wireless networks will be a necessity with the wide spread of wireless networks and limited geographic coverage and capacity of each network. In [1], we propose a super node system architecture based on the concept of delay tolerant network (DTN) to overcome roaming user intermittent connections over interconnected heterogeneous wireless networks. Mobile ad hoc networks play a key role in the super node system as it can provide a coverage for areas that lack a network infrastructure to bridge gaps between wireless networks within the system. Long delays combined with the lack of continuous communications with a network server introduces new challenges in information security for mobile nodes in a DTN environment. One of the major open challenges is to prevent unauthorized traffic from entering the network. This paper addresses this problem within the super node system. Two schemes are proposed: one is based on asymmetric key cryptography by authenticating the message sender, and the other is based on the idea of separating message authorization checking at intermediate nodes from message sender authentication. Consequently, the second scheme uses symmetric key cryptography in order to reduce the computation overhead imposed on intermediate mobile nodes, where one-way key chains are used. A simulation study is conducted to demonstrate the effectiveness of each scheme and compare the performance with and without using an authorization scheme. Moreover, the problem of secure end-to-end message exchanges is introduced by mapping the problem from a challenged network domain (i.e., among roaming nodes) to a reliable network domain (i.e., among super nodes over the Internet backbone). The proposed symmetric key based scheme is extended to achieve end-to-end security.**

***Index Terms*—End-to-end information security, prevention of unauthorized traffic, delay tolerant network (DTN), heterogeneous wireless networks, connectivity, intermittent links.**

I. Introduction

For ubiquitous networking, efficient internetworking among various types of wireless networks is essential. However, gaps in wireless network coverage and intermittent connections from/to a mobile node pose challenges in providing seamless service to roaming users. Our previous work [2] presents a super node based system that adopts the delay tolerant network (DTN) architecture to overcome these limitations.

The DTN architecture [3] is proposed to handle communications over challenged networks, which are characterized by long delays and frequent disconnections. It is based on an Internet-independent middleware, which handles sending and receiving of bundles (self contained messages) across the network using the underlying protocol stack. With a long end-to-end delay expected over a challenged network, DTNs cannot accommodate any real-time applications, but mainly support time insensitive applications. Message delivery in a DTN is done by first storing a message (i.e. bundle) and then forwarding it either to its destination or to an intermediate node that has a high probability to deliver it to the destination. For example, in the epidemic routing technique [4], each node forwards a received message to all its neighbor nodes. The message delivery mainly depends on node mobility, taking advantage that one of the message carriers may meet with the message's destination node.

Among challenges in a DTN due to long delays and frequent disconnections, one major open issue is how to limit unwanted (i.e., unauthorized) traffic within a network. The problem of preventing unauthorized traffic in regular networks is handled analogues to the problem of authentication, authorization and accounting (AAA). Authenticating user and assigning access privileges in traditional networks are performed by a special network node such as an access point in a wireless local area network (WLAN), a base station in a cellular network, or a network server in general. In a DTN, long delays and frequent disconnections make a continuous contact with such a network node impossible. As a result, a new scheme is required to cope with the new constraints.

In a DTN, an end-to-end route between the message source and the destination consists of a sequence of intermediate nodes in addition to the end nodes. These intermediate nodes can play a special role in the network such as message mules [5], [6] or they can be regular nodes [7]. The process of message delivery requires message storing and forwarding by intermediate nodes, which consumes network resources in terms of node buffer space and radio spectrum bandwidth. As a result, identifying and limiting unauthorized messages will reduce the overhead imposed

This paper is presented in part in a paper presented at IEEE Globecom 2009.

This work was supported by a Strategic Project Grant from the Natural Science and Engineering Research Council (NSERC) of Canada.

Manuscript received May 1, 2009; revised September 16, 2009; accepted September 30, 2009.

doi:10.4304/jcm.5.2.152-163

on the network. However, this requires the intermediate nodes to be able to authenticate the messages and verify message original sender's eligibility to use the network before accepting the message. There is no general solution proposed for this problem within the DTN architecture [8]. Most of existing solutions are highly specialized to a specific network scenario. For example, the work in [9] assumes that each node knows all eligible nodes' public keys. When a message is received, the signature is verified against all known eligible public keys. This technique is difficult to scale for a large heterogeneous network due to an expected huge number of nodes. Related techniques have been introduced for a vehicular network, such as the HAB (huge anonymous keys based) protocol [10]. The HAB protocol is to secure vehicular networks where each node possesses a huge set of keys to sign messages. There are many techniques that use the same idea of asymmetric key cryptography with a pre-distributed set of keys at each node (e.g., [11] and [12]), and the GSIS protocol [13] which does not require each node to store a huge number of keys. A problem with all these techniques is the extensive use of asymmetric key cryptography, which consumes a significant amount of resources in terms of time and computing power. This problem is addressed for vehicular networks in [14], where the proposed solution uses symmetric key cryptography, when a connection is available with a road side unit (RSU), to reduce the overhead.

Another major open issue in a DTN is how to secure end-to-end message exchanges. Unlike regular networks, it is difficult in a DTN environment to control message route. A malicious intermediate node that gets a copy of a message can disclose and/or change the message contents. As a result, end-to-end message security (i.e., message confidentiality and authenticity) is a necessity in a DTN. Secure end-to-end messages exchanges require mutual authentication between the communicating parties, i.e., the sender and receiver(s). In a large size network scenario, mutual authentication requires the communication with a trusted third party (e.g., certificate authority). Traditional techniques for end-to-end security cannot be applied directly to a DTN environment due to the potential unavailability of a physical end-to-end path either between the message's sender and the receiver or between each of them and a trusted third party. Without available communications with a trusted third party, communicating parties are not able to perform mutual authentication in a timely manner to allow the communication. There are some adaptations of regular techniques to handle this problem within a DTN, such as the work in [15] which proposes to use Identity Based Cryptography (IBC) and to adapt the regular public key cryptography to achieve secure end-to-end message exchanges. The main idea is to minimize the required communication with a trusted third party to overcome the unavailiabity of a continuous connection with the trusted third party. However, most of the proposed techniques are based of public key cryptography. In this paper, we propose a technique for achieving end-to-end secure message exchanges within the super node architecture, which employs symmetric key cryptography to reduce the computation overhead associated with public key cryptography. The main idea is to map the problem of mutual authentication from the unreliable network domain (i.e., between communicating nodes) to a reliable network domain (i.e., between super nodes).

This paper mainly investigates how to limit unauthorized traffic within a mobile ad hoc network (MANET) as a major component of the super node system. The proposed schemes are mainly adjusted to fit delay tolerant network based MANETs that serves as access networks within the super node architecture. However, the concept can be adapted to fit within different DTN scenarios. We adopt traditional public key infrastructure (PKI) based certificates to solve the problem under consideration. We also propose a new technique based on an idea of separating the message authorization and message sender authentication at intermediate nodes. The new technique uses symmetric key cryptography to reduce the overhead from that when using asymmetric key cryptography. Although the proposed technique is introduced within the super node system, it can be generalized to other DTN scenarios. We discuss how to achieve end-to-end message exchanges by extending the proposed approach. Our contributions can be summarized as five folds: i) Adopting traditional PKI based certificates for limiting unauthorized traffic within the super node system; ii) proposing the new idea of separating the problems of message sender authentication and message authorization at an intermediate node; iii) introducing a new technique based on symmetric key cryptography, employing the concept of one-way hash function, and introducing the concept of key group to reduce the overhead induced by asymmetric key cryptography techniques; iv) evaluating the performance of the proposed techniques over different routing techniques; and v) introducing the idea of moving the problem of mutual authentication to super nodes in order to reduce overhead imposed on the communicating mobile nodes.

The rest of this paper is organized as follows. Section II gives a brief overview of the super node system and a detailed description of the system model considered in this work. Section III presents the proposed solutions, section IV discusses how to achieve end-to-end security, and section V provides performance evaluation of the proposed solutions. Finally, section VI presents conclusions of this work.

II. The System Model

We consider a global information transport platform, which consists of a number of heterogeneous wireless access networks (e.g., cellular networks, mobile ad-hoc networks, WLANs, etc.) that are interconnected over an Internet backbone [16], as illustrated in Figure 1. Each network is connected to the Internet through a DTN gateway [3]. Each mobile node is able to connect to the

platform through a subset of the wireless access networks. A node may be connected for a period through one access network, disappear for an extended period, and then reappear from the same access network or from a different access network. Here, we focus on data communications for delay insensitive applications. To handle communication for this system, the super node architecture [2] is introduced. The super node architecture employs the concept of store and forward message exchange mechanism in DTN to provide reliable communication facilities for roaming users with intermittent connections. A roaming user can frequently encounter extended periods of disconnections and/or an intermittent connection with its current network, which causes the unavailability of an end-to-end stable communication path to the user. As a result, message exchange over the super node system is usually done through DTN bundles to achieve successful communication.

In the super node system, each super node is responsible for a set of users. Each user (mobile node) has a unique and fixed home super node, independent of its location changes. Communications among the super nodes and the gateways are assumed to be reliable and secure over the Internet. Each mobile node should contact its super node to update its location upon connecting to an access network. To send a message, the source node first locates the super node of the destination node based on user ID hashing. With the latest location update of the destination node provided by its super node, the source node then tries to establish an end-to-end connection with the destination. If the connection setup fails or the connection drops at any time, all the messages are sent to and stored at the destination super node for forwarding to the destination node upon its reconnection. To better illustrate the approach, consider a simple scenario as shown in Figure 1. Node A wants to send a message to node B. By hashing the ID of node B, it locates the super node S_B of node B. Node A sends to S_B a query about node B's location. Super node S_B sends to node A a message that contains the latest known location of node B. Then, node A tries to establish a direct connection to node B, which may be possible in some cases (e.g., if node B is connected through a WLAN or a cellular network) or may be infeasible (e.g., if node B is connected through a sparse ad hoc network with intermittent links). Suppose that node B is connected through a wireless ad hoc network. Node A first tries to establish a connection with node B directly, but fails; then node A sends the messages to super node S_B. Regardless of node B current access network, it is S_B's responsibility to deliver the messages to node B over the access network. Message exchanges between either nodes A and S_B or nodes S_B and B is not guaranteed to be delivered successfully, yet it depends on the current network condition and the employed routing technique.

The main function of DTN gateways is to provide the store and forward functionality over the existing network protocol stacks. For example, a DTN gateway is placed to interface between MANET and the Internet backbone.

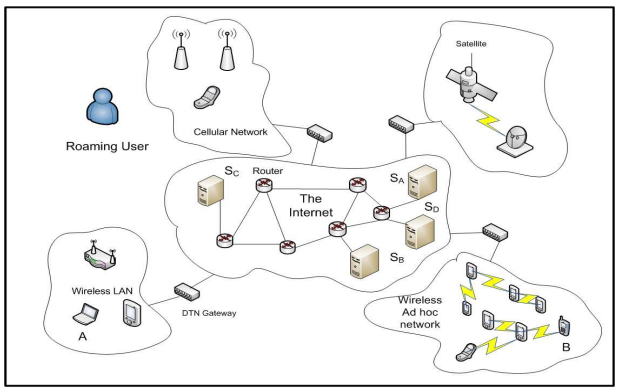

Fig. 1. The system architecture with super nodes.

Any message (i.e., bundle) sent over the MANET using its DTN routing protocol to a destination located in a different network should be forwarded and stored at the gateway. The gateway converts the received message to a suitable format for delivering it to the destination gateway using the underlying Internet protocols. When the message is received by the gateway in the destination network, it is converted by the gateway to a suitable format for delivering over that network (e.g., cellular network) to its destination. The gateway connection to the Internet backbone is assumed to be reliable and continuous. Each network should have its gateway that handles the message exchanges between the Internet and its network users. As a result, the number of gateways required will equal the number of end access networks. On the other hand, a super node is to function as a delegate for a set of users regardless of these users current access networks. The number of the super nodes will be a function of the total number of users, depending on many factors such as load balancing. The super node functions can be carried out by a server in the Internet that has the required capabilities with sufficient buffer space and processing power. As a result, a gateway can act as a super node too if it has the required capabilities. The super node architecture can be regarded as an adaptation of the super node concept in peer-to-peer networks (where a super node plays a special network role for regular peers [17]) to the DTN domain. More details about the super node system are given in [2].

There exist related schemes to handle communications with roaming users, such as in the terminodes project [18], yet they do not handle the potential intermittent connections to the users. The terminodes project is proposed to construct a huge self-organized network of mobile nodes. It is assumed that, with a large number of nodes, the node density is high. As a result, an end-to-end path is likely to exist between two communicating nodes. However, the super node architecture is concerned with the interconnection of heterogeneous wireless access networks to provide a continuous connection for a roaming user over the networks (e.g., cellular networks, MANETs, and WLANs). For MANETs within the super node system, it is assumed that the networks can be sparse so that

an end-to-end path between nodes within the network is unlikely. Communications in terminodes are based on assigning each node with a virtual home region (VHR). Each node should determine its geographical location and send this information back to all the nodes within its VHR. Any node wishing to communicate with this node should determine its location by contacting any node within its VHR and then forward its messages to this location. However, applying the technique to solve the problem under study in our research raises many issues: First, without availability of the destination node, the communication will not take place and/or the messages will be lost; Second, with the potential unreliability of the participating nodes, the node location information is not guaranteed to be stored reliably within the VHR; Third, due to the potential unreliable communication between nodes within the VHR, the location information stored within the nodes in VHR may be inconsistent; Finally, the VHR may happen to be empty of nodes at any time, which prevents the communication with all the associated nodes to be located. On the other hand, the super node architecture solves these issues by replacing the VHR with a reliable super node residing in the Internet, which acts as a communication delegate for the node, so that even with unavailability of the node itself the message delivery can still take place.

Preventing unauthorized traffic over the super node system implies preventing it over the access networks. However, within the super node system, some access networks already have a security infrastructure to prevent unauthorized nodes from using the networks such as cellular networks and secure WLANs. As a result, here we focus on wireless networks that do not have an infrastructure such as MANETs. The MANET model under consideration is shown in Figure 2, where the coverage of a MANET is limited to a geographical area. In the area resides a DTN gateway which connects the access network to the system. Within the MANET, there are a number of mobile nodes that can freely roam over the network coverage area. These nodes may have different communication capabilities in terms of wireless transmission range, memory size, and available transmission power. The nodes are free to enter (such as node E) or leave (such as node F) the area and consequently join or leave the network. A node can be unreliable as it can switch off at any time with or without a warning message. Two nodes are connected when they are able to communicate with each other, i.e., when they are within each other's transmission range. For simplicity, we assume that all nodes have the same transmission range and that, if node A can receive messages from node B, node B can receive messages from node A as well. We are interested in a situation where mobile nodes are sparsely distributed and the network is very likely to be partitioned, such that an end-to-end path rarely exists between a pair of communicating nodes.

The DTN gateway has a fixed location within the geographical area, with communication functions and capabilities similar to those of an ordinary mobile node. That is, the gateway is assumed to have a limited transmission range, and can communicate directly only with the nodes within its transmission range. The gateway transmission range covers only a small portion of the MANET geographical area. On the other hand, the gateway has higher processing power and larger storage (buffer) space than other roaming nodes. In terms of node mobility patterns, there is no restriction on node movements (except a reasonable upper bound on the velocity). An assumption is that some nodes usually roam toward the gateway, so that the gateway can communicate with the roaming nodes from time to time. This assumption can be satisfied by carefully choosing the gateway location, depending on the geographical features of the service coverage area.

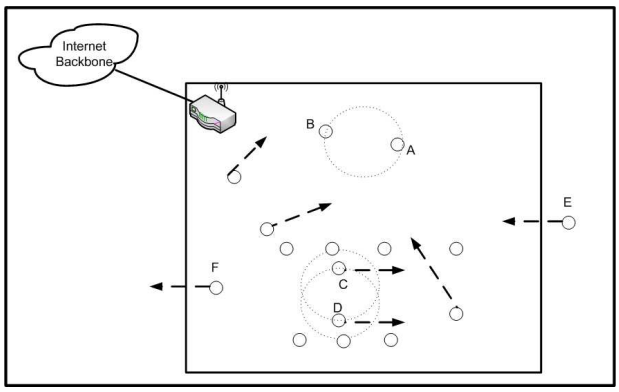

Fig. 2. An illustration of the MANET under consideration.

The role of granting network access to a mobile node should be assigned to a specific entity. This entity is determined based on the network under consideration. In our system model, the gateway grants network access to nodes currently connected through the network under its jurisdiction. The gateway is assumed to have no-knowledge about node private information such as passwords, current status, etc. In order to decide whether or not to grant access to a node, the gateway contacts the super node responsible for the node. The communication between the gateway and the super node is assumed to be reliable and secure over the Internet backbone. Each super node and the gateway have a public-private key pair. Each node should know the public key of its super node. Each node has a public-private key pair and the public key is stored at its super node.

III. The Proposed Security Schemes

Within the MANET access network, any roaming node can send a message over the network. Regardless of the sender, the intermediate nodes will carry and forward this message to either its destination (if it is within the network) or the gateway (if the destination is in another network). The main goal of this work is to prevent the messages of unauthorized users to be carried over the network. However, unauthorized nodes can roam over the network and participate (if they want) in message forwarding of other authorized nodes, yet they cannot

TABLE I
NOTATIONS

Notation	Description
ID_A	the public identifier of entity A
$\mid$	message concatenation operation
S_A	the super node of node A
PK_A	the public key of node A
SK_A	the private key of node A
$Enc_K(\cdot)$	symmetric key encryption function with key K
$Dec_K(\cdot)$	symmetric key decryption function with key K
K_i	symmetric key with index i
$E_X(\cdot)$	asymmetric key encryption function with key X
$D_X(\cdot)$	asymmetric key decryption function with key X
$H(\cdot)$	one-way hash function such as SHA-1
$H^i(\cdot)$	applying hash function H for i times
$HMAC_K(\cdot)$	a keyed-hash message authentication code, which is generated with symmetric key K
KG_n	a key group of length n

send their own messages. This assumption is based on the work introduced in [19] which argues that unauthorized nodes can help in delivering messages in the network as the unpredictable nature of a DTN reduces the effectiveness of tampering with message attacks to that of simple network failures. As a result, our goal is not to prevent unauthorized nodes from participating in message forwarding as data mules but to prevent them from being able to send their own messages over the network. One approach to solve the problem is to let intermediate nodes carry and forward a message regardless whether or not the sender is allowed to use the network resources (i.e., to send the message over the network). As the message reaches the gateway, the gateway can check the message sender and discard the message. This solution does not prevent unauthorized traffic, because message discarding occurs at the gateway after an unauthorized message has already been carried over the network and sometimes it may be delivered without going through the gateway. However, this approach moves the message checking process to the gateway, which reduces message checking overhead imposed on the intermediate nodes. On the other hand, with an increase of unauthorized messages, the network performance degrades (as to be discussed in Section V).

The two approaches proposed in the following depend mainly on attaching a message authentication code (MAC) block to each message. Using this block, any intermediate node can decide to carry the message or to discard it without the need to contact a third party. The difference between the two approaches is how to calculate the MAC block. The first approach is based on asymmetric key cryptography which is inefficient for the system model under consideration. As a result, the second approach is based on redefining the problem to separate the message authorization from the message sender authentication. The second approach uses symmetric key cryptography to reduce the overhead in the first approach. Table I summarizes the notations for easy reference.

A. PKI Certificate Based Scheme

The gateway is the node that can decide which user is eligible to use the network resources, i.e., it acts as a trusted third party. However, a continuous contact with the gateway from a mobile node is likely not possible within the system under consideration to allow the intermediate nodes to verify message sender eligibility to use the resources. One possible solution is to let the gateway act as a certificate authority which issues a PKI certificate for each authorized user.

When a node, A, first connects to the network, it should contact its super node, S_A. This connection message must travel through the gateway to reach the super node:

$$ConnectMsg \leftarrow ID_A \mid ID_{net} \mid TimeStamp \mid SIG_A,$$
$$SIG_A \leftarrow E_{SK_A}(H(ID_A \mid ID_{net} \mid TimeStamp)).$$

Based on the connection message, the super node can authenticate the user identity and inform the gateway whether or not this user should be granted access over the network and the period of granted access. As the super node knows the node public key, it constructs a permission message and sends it back to the gateway:

$$PermMsg \leftarrow ID_A \mid ID_{net} \mid Duration \mid TimeStamp \mid PK_{gateway} \mid PK_A \mid SIG_{S_A},$$
$$SIG_{S_A} \leftarrow E_{SK_{S_A}}(H(ID_A \mid ID_{net} \mid Duration \mid TimeStamp \mid PK_{gateway} \mid PK_A)).$$

As the node does not know the public key of the gateway, the super node includes the gateway public key in the permission message to authenticate the gateway. The gateway uses this message and issue a temporary certificate to grant the node access to the network:

$$Cert_A \leftarrow ID_A \mid ID_{net} \mid ExpTime \mid PK_{gateway} \mid PK_A \mid SIG_{gateway},$$
$$SIG_{gateway} \leftarrow E_{SK_{gateway}}(H(ID_A \mid ID_{net} \mid ExpTime \mid PK_{gateway} \mid PK_A)).$$

The node checks the authenticity of the certificate by checking the permission message. To send a message over the network, the node signs the message with its private key and sends the signed message with the certificate. Intermediate nodes can check the message authenticity by checking the certificate. This implies that each intermediate node performs two asymmetric operations per carried message, one to check the message signature and the other to check the certificate itself. Based on the routing technique used, the intermediate node forwards the message with its certificate attached.

Limiting the certificate live time overcomes the problem of certificate revocation in order to revoke node access. Upon certificate expiration, the node can recontact the gateway to request more network access time. The problem with this approach is the overhead imposed by the required number of asymmetric operations. A message sender should sign the message in order to forward it. Each intermediate node receiving the message should verify the signature and the sender's certificate, which requires two asymmetric decryption operations per message. With a large number of messages, this can

represent a overwhelming overhead, considering power limited portable devices.

B. Symmetric Key Based Scheme

This main proposed technique uses symmetric key cryptography to reduce the number of required asymmetric operations and hence the imposed overhead. The technique uses the concept of one-way key chain [20]. One-way key chain is a sequence of keys generated by consecutive applications of a one-way hash function. Figure 3 shows the generation of a one-way key chain

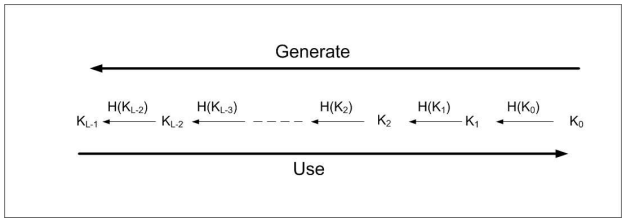

Fig. 3. One-way key chain of length L.

with a seed key K_0, which is randomly chosen. The chain is generated by consecutive applications of one-way hash function $H(\cdot)$ to the seed value (i.e, key). Any key K_x can be used to reveal any subsequent key K_y, where $y > x$. By the one-way hash function definition, a key K_y cannot be used to obtain a key K_x where $x < y$, because this implies to reverse the one-way hash function. As a result, the direction of key usage, in the chain, is in the reverse direction of the key generation. For example, for a key chain of length L with initial key K_0, the generation requires applying the hash function H for $L-1$ times; but the first key to use is K_{L-1}, the second key is K_{L-2}, and so on. To generate a key K_i, the hash function should be repeatedly applied for i times on the seed key:

$$H^i(K_0)=K_i, \qquad 0 < i < L.$$

The introduced idea is based on the fact that the asymmetric key cryptography based technique not only proves the message legitimately, but also authenticates the sender identity which is not required in the problem under consideration. The authentication of the sender identity should be a problem of the message destination (not intermediate nodes), which is part of the process of establishing end-to-end security. Intermediate nodes need only to ensure that any received message is authorized to be carried over the network, but not to prove the identity of its sender. With a symmetric key to compute a message signature using a key hashing algorithm, only authorized nodes should know the key that will be regularly updated by the network gateway. The network access time assigned to a node varies depending on the node, similar to the certificate live time. The gateway can generate a set of keys, and each key is to be used within a time frame in the network. Nodes check each received message against the key used when the message were issued based on the message time stamp. Due to potential long delays in message delivery, existing messages may belong to different time frames and consequently different keys. This requires that a new node should receive not only the keys that cover its network access period but also old keys to participate in message forwarding. This is solved by employing the concept of one-way key chain.

The network gateway generates a key chain to be used over a long time period. The gateway splits the time period into equal durations (frames), and each key in the chain is used for a specified duration. Based on how long a node is permitted to access the network, a subset of the chain (*key group*) is shared with the node. To send a message, the sender node generates a MAC block using a key based on the message time stamp. Intermediate nodes check the MAC block against the shared key chain to check if the message is legitimate to be carried or not.

When a node, A, connects to the ad hoc network supervised by gateway G, it sends a connection message to its super node. When the super node receives the message, it sends a permission message to the gateway. The gateway grants network access to this node for a specific time period by sending a key group that covers this period. For example, if the key live time is t_{key}, and the gateway wants to grant an access period of $5t_{key}$, then the gateway should send the current key and the next 4 keys to the node. We call the keys *key group* (KG). If the current key is K_x, the key group of size n is a concatenation of n key:

$$KG_n \leftarrow k_x \mid k_{x-1} \mid \ldots \mid k_{x-n+1}.$$

To reduce the message size, the gateway does not need to send all the keys in the key group, but only the last key K_{x-n+1} in the group and the group length. The node can generate the group by consecutively applying the hash function. The gateway generates the network access message by encrypting the key group with the node public key:

$$AccessMessage \leftarrow E_{PK_A}(KG_n \mid TimeStamp).$$

After verifying the access message and the permission message, the node gets the key group and starts communicating over the network.

It should be noted that the node can generate all the keys that precede the first key in the key group (using the hash function). It is expected that the messages already circulating in the network are encrypted using previous keys, so that the node can verify the validity of these messages. The node cannot generate any key for a future time period using the key group based on the one-way key chain properties. For example, the node that received a key group KG_n with current key K_x can generate any previous key K_i where $L-1 \leq i < x$. If a node needs to communicate over the network after the expiry of its key group, it should re-register with the gateway.

After obtaining the key group, the node can start communicating with other nodes. When the node wants to send a message, it needs to generate a MAC block using the current network key and forwards it to neighbor nodes (based on the routing technique applied). The message

exchanges are in the form of

$$ExchangedMsg \leftarrow Msg \mid TimeStamp \mid MAC,$$
$$MAC \leftarrow HMAC_{K_x}(Msg \mid TimeStamp).$$

When an intermediate node receives a message, it checks the MAC block and then stores the message to be forwarded. The intermediate node is not able to disclose the message contents because the message Msg should already be encrypted with another key shared between the source and the destination to achieve end-to-end secure communications, as discussed in Section IV.

To prevent any node from continuing the communication with a previously granted key group, messages sent with expired keys are discarded as follow: Key K_i has a time frame $[t_x, t_x + t_{key}]$ and each message has a live time $t_{message}$. If a message at time $t > t_x + t_{key} + t_{message}$ is authorized with key K_i, it will be discarded.

With the proposed approach, a message sender needs to perform one symmetric key encryption per message. Each intermediate node also needs to perform one symmetric key decryption per message. Intermediate nodes store the original message (if valid) for future forwarding. They do not need to re-compute the message MAC when forwarding the message.

IV. End-to-End Message Security

Preventing unauthorized users from sending their messages over the network does not implies the confidentiality of exchanged authentic messages. Any malicious node that receives a message for forwarding can expose the message contents. Due to the inability to control the message forwarding route within the system under consideration (especially for an unstructured open network such as MANET), secure end-to-end message exchanges are mandatory.

In the system under consideration, the existence of super nodes that can communicate reliably and securely over the Internet backbone offers an advantage to relax the constraints of end-to-end secure message exchanges. The main idea is to use the super node as a node delegate that performs the mutual authentication and key sharing on behalf of the mobile node. Under the super-node architecture, there are two communication scenarios for node-to-node message exchanges: 1) the message sender and receiver can find a physical end-to-end path, and 2) a physical end-to-end path cannot be established, so that messages are routed through the destination's super node. In both cases, the source node should contact the destination's super node. For the first case, the source node has to contact the destination's super node to locate the destination, while in the second case all messages are sent through the super node.

We propose to use symmetric encryption to ensure information security for communications between a node and its super node. All message exchanges are encrypted using a shared secret key, which reduces the overhead imposed by asymmetric cryptography based techniques. The shared key is updated periodically to prevent its exposure. Updating the shared key requires handshaking between the node and its super node, which is challenging with the expected node's frequent long disconnections. To handle key updates, a key chain is shared between the node and its super node. The key chain is used for a period of time which is divided into time frames of equal length and, for each time frame, a specific key from the chain is used to secure the communications. At the end of a time frame, both the node and its super node update the shared key to the next key from the key chain without the need of any handshaking between them. After all the keys from the chain are used, a new key chain will be generated and shared between the node and its super node. This technique does not need to include the secret key in the exchanged messages as in traditional asymmetric cryptography based techniques. Asymmetric cryptography is used only during the chain initialization to securely exchange the key chain and to allow the communicating parties to authenticate each others, as discussed next.

When a node, A, is connected through an access network, it sends a connection message to its super node to update the super node with its current location and to be granted the privilege to access the access network resources as discussed in Section III. If there is no shared key chain or a previously shared chain expired, node A initializes a new chain by generating a random key as the chain seed value K_0 and length L. The node prepares the connection message as:

$$ConnectMsg \leftarrow ID_A \mid ID_{net} \mid E_{PK_{S_A}}(K_0 \mid L) \mid TimeStamp \mid SIG_A,$$
$$SIG_A \leftarrow E_{SK_A}(H(ID_A \mid ID_{net} \mid E_{PK_{S_A}}(K_0 \mid L) \mid TimeStamp)).$$

The access network identifier ID_{net} is to inform the super node of its current location. The connection message contains a time stamp field to prevent a reply attack. The key chain information is encrypted with the super node public key to ensure that only the super node can decrypt this information. The node signs the message with its private key to enable the super node to authenticate the sender identity. The super node verifies the connection message and initializes the key chain. The super node sends access information to the node as discussed Section III. The node and its super node can start exchanging messages secured with the current shared key, K_i, from the shared key chain:

$$ExchangedMsg \leftarrow (Enc_{K_i}(msg \mid TimeStamp) \mid i).$$

The node does not have to initialize a new key chain until all the keys in the current key chain are used. This allows the node to be disconnected from its super node while keeping an up-to-date shared key without any handshaking between them.

Due to the expected delay in message delivery, messages may not be delivered in sequence. Hence, the receiver (i.e., the node or its super node) may receive

messages encrypted with the keys out of order, or with previous keys other than the current key. The proposed technique addresses this potential problem by including a time stamp in the message. The receiver accepts the message as long as the key index matches the enclosed time stamp.

To establish a secure end-to-end message exchange between two nodes, our proposal is to use the destination node's super node as the destination's delegate. This moves the mutual authentication process from the communicating nodes (where the communication is challenged) to their super nodes (where the communication is reliable and secure). The first step for communications between two nodes is that the source node inquiries about the destination node location from the destination node's super node. This step can be used to enable the destination super node to authenticate the source node identity. The destination super node issues a permission for secure communication in the form of an access ticket that the source node can use to communicate with the destination node. With the access ticket, the destination node does not need to re-authenticate the source node as the ticket proves that the sender is authenticated by the destination super node. Moreover, the source node does not need to authenticate the destination node because the destination node is the only one who can extract the shared key information from the ticket.

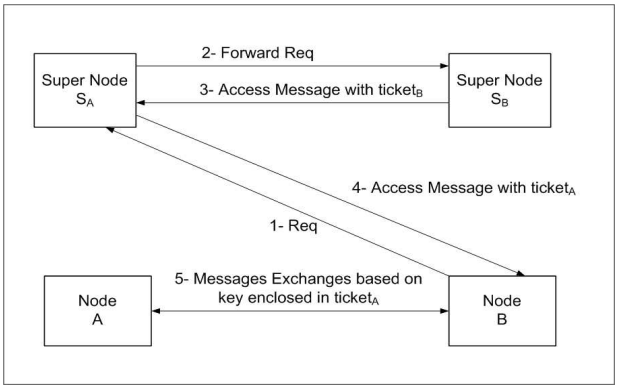

Fig. 4. The procedure to establish an end-to-end secure message exchange.

Figure 4 shows the proposed procedure to establish a secure end-to-end message transfer between two nodes. Suppose that node B wants to start a secure communication with node A. Node B locates the super node S_A and sends a communication request, Req, to S_A as follow:

$$Req \leftarrow (ID_A \mid ID_B \mid TimeStamp \mid \underbrace{i \mid Enc_{K_i}(ID_A \mid ID_B \mid TimeStamp)}_{AuthenticationPart}).$$

The authentication part in the request message is encrypted by the current shared key between node B and its super node. If S_A is not the super node of node B, it cannot authenticate the sender identity. As a result, it forwards the request message to node S_B (based on the assumption that super nodes can communicate reliably and securely over the Internet backbone). Node S_B verifies that node B is the sender of this message based on their shared key chain and generates *access ticket* $ticket_B$ to S_A for a secure communication with node B. Super node S_B replies to S_A with an access message that is secured based on the assumed existing secure connection between the super nodes:

$$ticket_B \leftarrow i \mid Enc_{K_i}(ID_A \mid ID_{S_A} \mid K_B \mid TimeStamp \mid ExpirationTime),$$
$$AccessMsg \leftarrow K_B \mid ExpirationTime \mid ticket_B.$$

The access ticket $ticket_B$ can be used only by node A and/or its super node S_A, which is declared as a part of the ticket. The ticket also contains a randomly generated secret key K_B to secure the communications with node B. The ticket is valid for a period of time determined by $ExpirationTime$ field. The access ticket $ticket_B$ authenticates both nodes A and S_A identities to node B. When S_A receives the access message that confirms the identity of node B, it generates an access ticket ($ticket_A$) using the current key, K_j, from the key chain shared with node A. Super node S_A sends an access message to node B that contains node A location and $ticket_A$:

$$ticket_A \leftarrow j \mid Enc_{K_j}(ID_B \mid ID_{S_B} \mid K_B \mid TimeStamp \mid ExpirationTime)$$
$$AccessMsg \leftarrow Location_A \mid ticket_B \mid Enc_{K_B}(ExpirationTime \mid ticket_A).$$

When node B receives the access message, K_B can be extracted from the ticket $ticket_B$ using K_i. Node B can start communicating with node A or its super node (if no end-to-end path exists). Each message msg sent from node B to node A is encrypted using the shared key K_B. An exchanged message includes the encrypted message and the access tickets, given by

$$ExchangedMsg \leftarrow Enc_{K_B}(msg) \mid ticket_A \mid ticket_B.$$

When node A receives the message, it checks $ticket_A$ using K_j, and then it decrypts the message using K_B obtained from the ticket. Note that, unlike the previous techniques [15], a message receiver does not need to authenticate the message sender and it can decrypt the message without any delay or asymmetric cryptography overhead. Moreover, node A can reply to node B using $ticket_B$ so that the communication proceeds without any need to contact the super nodes again for authorization.

To prevent using expired tickets in communications, messages sent with expired tickets are discarded as follow: Given that the ticket expiration time t_{ticket} and each message has a live time $t_{message}$, if a message using this ticket is received at time $t > t_{ticket} + t_{message}$, the message will be discarded.

A main challenge for authentication over DTN is the delay required for handshaking to complete the authentication process. In our scheme, the delay is minimized by using the mandatory message sent to the super node to locate the destination node. As a result, the sender does

not need to send a separate message for authentication. Moreover, within the lifetime of the issued ticket, the sender does not need to re-send an authentication message for each message. Note that there exist some research efforts to provide a self organized authentication without the need to contact a trusted third party, such as the work in [21]. The technique is based on the self signed certificates issued by the nodes themselves. A main concern for the technique to be adapted to the super node architecture is the size of required certificate repositories within each node, taking into consideration the huge interconnected networks. The authentication requires processing a graph of the intersection among the node certificate repositories, which can be huge for roaming nodes with a possibility of no shared certificates. With the expected unavailability of the communicating nodes and/or an end-to-end path, the handshaking required for the authentication (i.e., to exchange the certificates) can either cause a long delay for the communication or prevent the communication completely. As it is the responsibility of the nodes to authenticate each other, the existing technique imposes a processing overhead to all the nodes.

V. Performance Evaluation

A. Routing over the Super Node Architecture

Routing over the super node architecture can be regarded on two levels. The high level routing is among super nodes and gateways, while the lower level routing is between end user(s) and the gateway over the access network. Communication among super nodes and gateways is assumed to be reliable and secure over the Internet backbone. The super nodes and gateways are assumed to have fixed locations over the Internet. As a result, message routing among them can base on the regular Internet routing. When an end user sends a message over an access network, the message is routed over the access network (to be discussed in the following) to the network gateway. The gateway forwards the message to the destination user's super node over the Internet backbone. The super node then forwards the message to the gateway of the destination user's current access network.

Routing over an access network is a challenge because of the potential unavailability of the destination node. It highly depends on the access network. For infrastructure based networks (e.g., cellular networks, and WLAN), regular routing techniques can be applied when the destination user is available. For example, in cellular networks, successful message delivery can be achieved by forwarding the message to the base station through which the destination user is currently connected. Routing becomes more complicated for infrastructure-less networks (e.g., MANETs), due to the potential unavailability of a physical end-to-end path between the gateway and the destination user over such networks.

We study how the proposed security schemes affect system performance under two different routing techniques: the epidemic routing [4] and the dominating set (DS) based routing [7]. In the epidemic routing, each node forwards a message to all its neighboring nodes, in anticipation that one of these nodes may meet with the destination node in the near future as it roams. This may be inefficient in terms of network resource usage, however it is sometimes necessary. On the other hand, the DS routing limits the number of forwarded messages required to deliver a message by limiting the number of nodes to which the message should be forwarded by a node. The DS routing counts on forwarding the message only to the DS members, which are nodes that have a high probability to meet with all the other nodes in the network.

B. Node Mobility Model

Node mobility model is one of the main concerns in DTN simulation [22]. Our following mobility model used in the simulation intends to make a compromise between simplicity and practicality. The geographical area covered by the MANET is partitioned to m partitions. When a node is connected to the network, it visits each of the partitions with a certain probability. The location of a mobile node in the future is independent of its location in the past, given its current location. Denote the location state of a mobile node by the partition it resides, and assume that the residence times of all the mobile nodes in each partition are iid exponential random variables. Then, the user mobility model can be characterized by a one-dimensional continuous-time Markov chain, with location state space $\{1, 2, \ldots, m\}$, as shown in Figure 5.

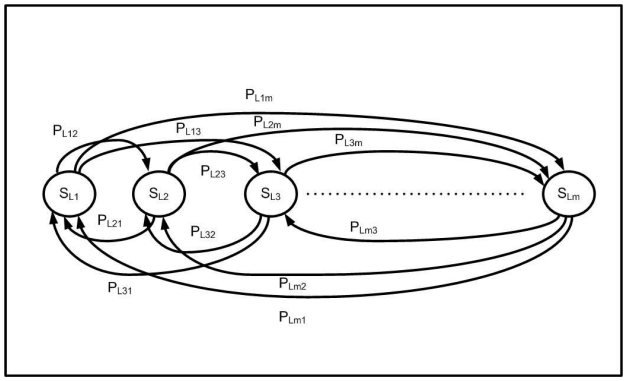

Fig. 5. Modeling of node movement by a finite-state Markov chain.

The user movement model over the network coverage area is described by the transition matrix M of the Markov chain, given by

$$\mathbf{M} = \begin{pmatrix} P_{L_{11}} & P_{L_{12}} & \cdots & P_{L_{1m}} \\ P_{L_{21}} & P_{L_{22}} & \cdots & P_{L_{2m}} \\ \cdots & \cdots & \cdots & \cdots \\ P_{L_{m1}} & P_{L_{m2}} & \cdots & P_{L_{mm}} \end{pmatrix}$$

where $P_{L_{ij}}$ is the conditional probability that a mobile node will enter partition L_j given that it is still connected to the network and it leaves its current partition L_i. For any partition L_i, we have $\sum_j P_{L_{ij}} = 1$. The transition probability matrix depends on the geographical characteristics of the service area and the network environment under study.

C. Simulation Results

We compare the performance of the proposed authorization techniques with that of the system with no authorization. The performance is measured in terms of (1) the number of forwarded messages over the network to demonstrate how efficiently each technique uses the available resources (e.g., radio spectrum bandwidth), and (2) the number of undelivered authorized messages to indicate how reliable the technique is in delivering authorized messages. We compare the two proposed security techniques in terms of the number of asymmetric key operations to measure how efficient the intermediate node computing power is used, with an increasing number of forwarded messages.

In our experiments, the MANET coverage area is a rectangle of size $1500m \times 1500m$. The area is partitioned into 100 $150m \times 150m$ partitions. Each simulation proceeds in discrete time steps. There are 50 mobile nodes with mobility trajectories independent of each other. For each simulation run, a transition matrix M is randomly generated and stays fixed till the end of the simulation. Initially, the node locations are uniformly distributed over the service area. As the simulation time increases, each node (if connected) moves randomly according to the transition matrix. When a node moves to a new partition, it stays there for a residence time that is an exponential random variable with an average of 20 simulation steps. At the end of the residence time, the node moves to a new partition with a probability of 0.7, or disconnects from the network with a probability of 0.3. If the node disconnects, it will stay disconnected for a duration that is exponentially distributed with an average of 20 time steps. For simplicity, we assume that a node is able to communicate only with other nodes in the same partition. Messages are generated based on a Poisson process with mean rate of $\frac{10}{3}$ messages per time step. The source and destination mobile nodes for each message are selected at random. All the messages are equal in size, with the same message live time of 40 simulation steps. The buffer space is 15 messages at each mobile node and 2000 messages at the gateway. When the node buffer is full and a new message is received, the oldest message in the buffer is removed to accommodate the new message. Moreover, 20 percent of the nodes are unauthorized to use the network resources. They are assumed to behave honestly in carrying and forwarding messages from others. In addition, they generate their own messages and try to inject them to the network.

At the start of simulation, all the nodes generate a request message to the gateway to gain access to the network based on the proposed security scheme (i.e., they receive a certificate in the first approach or a key group in the second approach). All the nodes are granted the same access period for simplicity in simulation. When the access period of a node expires, the node has to re-request access from the gateway. At each time step, the node detects its neighbor nodes and exchanges the buffered messages with them (the messages that the neighbor nodes do not already have) based on the routing technique. Each node also updates its buffer by removing expired messages. For each experiment, a communication scenario (i.e., set of messages, user connections, user disconnections, user movements) is set up randomly and run for each scheme.

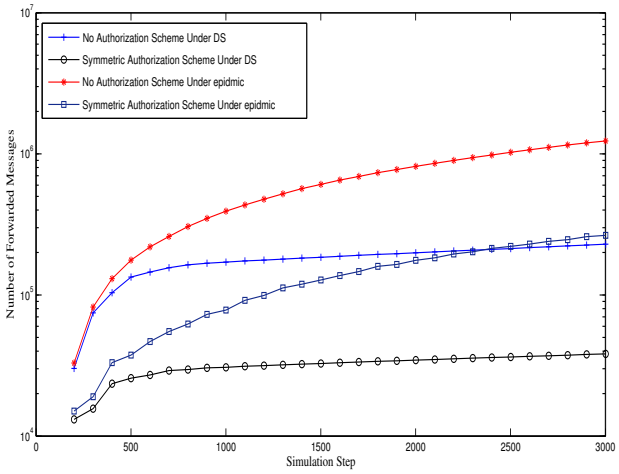

Fig. 6. Comparison of the proposed authorization schemes in terms of the number of forwarded under the DS and the epidemic routing.

Figure 6 shows a comparison between the case of applying no authorization scheme and the case of applying the proposed symmetric key cryptography based authorization scheme under the epidemic routing and DS routing, in terms of the total number of forwarded messages. It is clear that, with the existence of unauthorized traffic, the authorization scheme is important to reduce the number of forwarded messages. This applies to both routing techniques under consideration. Moreover, the number of lost (undelivered) authorized messages is highly increased in the case of no authentication, as shown in Figure 7. This is mainly due to the limited buffer space at intermediate nodes which have to drop old messages when buffer overflow occurs. With an increasing number of unauthorized messages, the probability of dropping authorized messages increases.

Both of the proposed authorization techniques perform equally in terms of the numbers of forwarded messages and lost messages. However, when comparing them regarding the number of asymmetric key cryptographic operations, it is clear that the symmetric key based cryptography outperforms the asymmetric key cryptography based scheme under the routing techniques, as shown in Figure 8. It should be noted that the symmetric key cryptography based scheme does not eliminate the usage of asymmetric key cryptographic operations as a node has to perform asymmetric key operation to request network access and to receive the key group (if access granted), as discussed in Section III-B. However, with a larger network size (in terms of number of nodes) and/or a shorter granted access period per node, even though the symmetric key cryptography based scheme increases the number of the required asymmetric key cryptographic

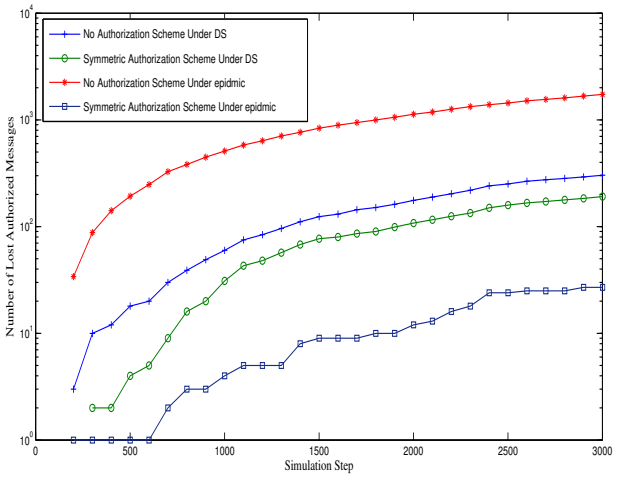

Fig. 7. Comparison of the proposed authorization schemes in terms of the number of lost authorized messages under the DS and the epidemic routing.

operations, it still outperforms the other scheme. This is mainly because the asymmetric key cryptography based scheme is affected by the same factors as well. As a result, it is expected that the symmetric key cryptography based technique always outperforms the asymmetric key cryptography based technique in terms of the number of asymmetric key cryptographic operations under all conditions.

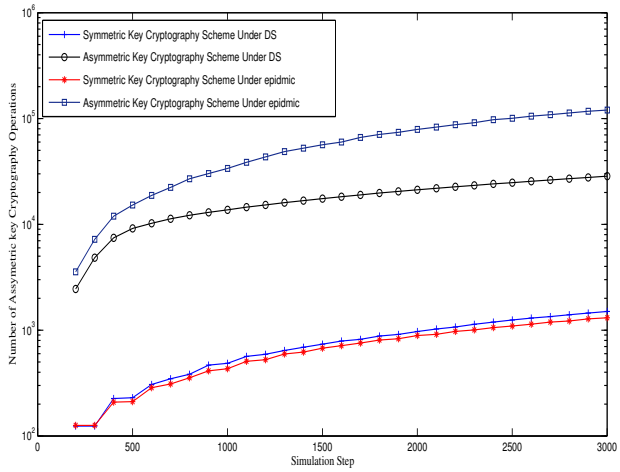

Fig. 8. Comparison of the proposed authorization schemes in terms of the number of asymmetric key cryptography operations under the DS and the epidemic routing.

Comparing the performance of the two routing techniques under the proposed authorization scheme, Figure 6 shows how the DS routing outperforms the epidemic routing in terms of the number of forwarded messages, which is consistent with the observation in the absence of unauthorized traffic [7]. In the presence of unauthorized traffic, even without the authorization, the DS routing outperforms the epidemic routing, as the DS routing limits the number of nodes that a message should be forwarded to. On the other hand, Figure 7 shows that, with the authorization scheme in place, the epidemic routing outperforms the DS routing in terms of the number of lost authorized messages. With the DS routing, a message is more likely to be expired before a contact occurs between a message carrying node and the next DS member. However, the number of lost authorized messages under the DS routing and the authorization scheme is much smaller than that under either the epidemic routing or the DS routing without the authorization scheme.

Considering the number of asymmetric key cryptography operations, the DS routing outperforms the epidemic routing, when asymmetric key cryptography based scheme is employed, as shown in Figure 8. This is because the number of asymmetric key cryptography operations is related to the number of message forwarded in the asymmetric key cryptography based scheme. However, the epidemic routing and DS routing perform similarly in terms of the number of asymmetric key operations performed, when the symmetric key cryptography based scheme is employed. This is due to the fact that the number of asymmetric key operations in this case is proportional to the number of connection messages and permission messages sent over the network. The higher number of lost messages in the DS routing likely results in more lost connection messages and/or permission messages, which requires the recalculation and resending of these messages.

We have carried out extensive simulations to evaluate the performance of the proposed schemes. The main observations can be summarized in the following: (a) Both schemes introduce an extra delay for a newly connected node to be able to communicate in the network. This delay accounts for the time for the access request to reach the gateway and the time for the node to receive the access grant information (key group or certificate). However, even with a highly sparse network, the simulation results show that the delay can be neglected when compared with the node connection time for the system model under consideration; (b) Both proposed schemes introduce extra cost as compared with the case of no authorization procedure. This cost is in the form of extra message exchanges to request and grant node access and the delay that a node encounters for accessing the network. This cost becomes obvious with a very low percentage of unauthorized messages. However, the overhead imposed by an increase in unauthorized traffic makes the extra message exchanges totally negligible; (c) When a node needs to extend its network access period, it sends a request message to the gateway. This introduces a delay until the response is sent back. The delay can be eliminated by requesting access in advance before the current access period is expired. The advance period can be estimated based on the average message delay that a node encounters in contacting the gateway.

VI. Conclusions

This paper investigates information security in the DTN based super node system. We propose two schemes for preventing unauthorized traffic in the MANET. The

first one is based on the conventional asymmetric key cryptography that solves the problem by authenticating the message sender. The second scheme is based on the idea of separating the issue of traffic authorization from the issue of message sender authentication at intermediate nodes. Using the symmetric key cryptography, the scheme is based on the concepts of key chain and key group. We also addresses the issue of end-to-end secure message exchanges over the super node system, based on the key chain concept. The proposed scheme moves the mutual authentication phase from mobile nodes to their super nodes for fast and reliable implementation. Computer simulation results demonstrates that 1) the proposed schemes achieve better utilization of the network resources by limiting unauthorized traffic, 2) the symmetric key based scheme outperforms the asymmetric key based scheme in terms of intermediate node computing power saving, and 3) the dominating set based routing outperforms the epidemic routing under the proposed information security scheme, in terms of the required number of forwarded messages, at the cost of increased number of lost messages and a slightly increased number of asymmetric key cryptographic operations.

ACKNOWLEDGMENT

The authors would like to thank Dr. Bruno Preiss of the Research In Motion (RIM) for many helpful discussions on this research.

REFERENCES

[1] H. Samuel, W. Zhuang, and B. Preiss, "DTN based dominating set routing for MANET in heterogeneous wireless networking," *Mobile Networks and Applications*, vol. 14, pp. 154 – 164, April 2009.

[2] H. Samuel, W. Zhuang, and B. Preiss, "Routing over interconnected heterogeneous wireless networks with intermittent connections," in *Proc. IEEE ICC '08*, pp. 2282 – 2286, May 2008.

[3] K. Fall, "A delay-tolerant network architecture for challenged internets," in *Proc. ACM SIGCOMM '03*, pp. 27–34, 2003.

[4] A. Vahdat and D. Becker, "Epidemic routing for partially connected ad hoc networks," April 2000. [Online]. Available: citeseer.ist.psu.edu/vahdat00epidemic.html

[5] W. Zhao and M. H. Ammar, "Message ferrying: proactive routing in highly-partitioned wireless ad hoc networks," in *Proc. IEEE FTDCS '03*, pp. 308–314, 2003.

[6] W. Zhao, M. Ammar, and E. Zegura, "A message ferrying approach for data delivery in sparse mobile ad hoc networks," in *Proc. ACM MobiHoc '04*, pp. 187–198, 2004.

[7] Hany Samuel, W. Zhuang, and B. Preiss, "DTN based dominating set routing technique for mobile ad hoc networks," in *Proc. QShine '08*, July 2008.

[8] S. Farrell, S. Symington, H. Weiss, and P. Lovell, "Delay-tolerant networking security overview," *IRTF, DTN research group*, February 2008.

[9] K. Ren, W. Lou, and Y. Zhang, "Multi-user broadcast authentication in wireless sensor networks," in *Proc. IEEE SECON '07*, pp. 223–232, June 2007.

[10] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.

[11] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. IEEE INFOCOM 2008*,pp. 1229–1237, April 2008.

[12] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proc. IEEE INFOCOM 2008*, pp. 246–250, April 2008.

[13] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: a secure and privacy-preserving protocol for vehicular communications," *IEEE Trans. Vehicular Technology*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.

[14] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: An efficient rsu-aided message authentication scheme in vehicular communication networks," in *Proc. IEEE ICC '08*, pp. 1451–1457, May 2008.

[15] N. Asokan, K. Kostiainen, P. Ginzboorg, J. Ott, and C. Luo, "Applicability of identity-based cryptography for disruption-tolerant networking," in *Proc. ACM MobiOpp '07*, pp. 52–56, 2007.

[16] H. Jiang, W. Zhuang, and X. Shen, "Cross-layer design for resource allocation in 3G wireless networks and beyond," *IEEE Communications Magazine*, vol. 43, no. 12, pp. 20–126, Dec. 2005.

[17] V. Lo, D. Zhou, Y. Liu, C. GauthierDickey, and J. Li, "Scalable supernode selection in peer-to-peer overlay networks," in *Proc. Second International Workshop on Hot Topics in Peer-to-Peer Systems*, pp. 18–25, July 2005.

[18] J.-P. Hubaux, T. Gross, J.-Y. Le Boudec, and M. Vetterli, "Toward self-organized mobile ad hoc networks: the terminodes project," *IEEE Communications Magazine*, vol. 39, no. 1, pp. 118–124, Jan 2001.

[19] J. Burgess, G. D. Bissias, M. D. Corner, and B. N. Levine, "Surviving attacks on disruption-tolerant networks without authentication," in *Proc. ACM MobiHoc '07*, pp. 61–70, 2007.

[20] A. Perrig, R. Canetti, D. Tygar, and D. Song, "The TESLA broadcast authentication protocol," 2002. [Online]. Available: citeseer.ist.psu.edu/perrig02tesla.html

[21] J.-P. Hubaux, L. Buttyán, and S. Capkun, "The quest for security in mobile ad hoc networks," in *Proc. ACM MobiHoc '01*, pp. 146–155, 2001.

[22] P. Luo, H. Huang, W. Shu, M. Li, and M.-Y. Wu, "Performance evaluation of vehicular DTN routing under realistic mobility models," in *Proc. IEEE WCNC 2008*, pp. 2206–2211, April 2008.

Hany Samuel received the B.Sc. degree in 2001 and the M.Sc. degree in 2006, both in electrical engineering, from Ain Shams University, Cairo, Egypt. He is currently working toward his Ph.D. degree at the Department of Electrical and Computer Engineering, University of Waterloo, Ontario, Canada. His current research interests include interworking of heterogeneous wireless networks, delay tolerant networks, and peer-to-peer systems. He is a co-recipient of a Best Paper Award from ICST QShine 2008.

Weihua Zhuang received the B.Sc. and M.Sc. degrees from Dalian Maritime University, China, and the Ph.D. degree from the University of New Brunswick, Canada, all in electrical engineering. Since October 1993, she has been with the Department of Electrical and Computer Engineering, University of Waterloo, Canada, where she is a Professor. She is a co-author of the textbook Wireless Communications and Networking (Prentice Hall, 2003). She is a co-recipient of a Best Paper Award from IEEE ICC 2007, a Best Student Paper Award from IEEE WCNC 2007, and the Best Paper Awards from Int. Conf. Heterogeneous Networking for Quality, Reliability, Security and Robustness (QShine 2007 and 2008). Her current research interests include wireless communications and networks, and radio positioning. Dr. Zhuang received the Outstanding Performance Award in 2005, 2006, and 2008 from the University of Waterloo for outstanding achievements in teaching, research, and service, and the Premiers Research Excellence Award (PREA) in 2001 from the Ontario Government for demonstrated excellence of scientific and academic contributions. She is the Editor-in-Chief of IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, and an Editor of IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, EURASIP JOURNAL ON WIRELESS COMMUNICATIONS AND NETWORKING, and INTERNATIONAL JOURNAL OF SENSOR NETWORKS. She is a Fellow of the IEEE and an IEEE Communications Society Distinguished Lecturer.