Journal of Information Processing Vol.25 234–243 (Feb. 2017)

[DOI: 10.2197/ipsjjip.25.234]

Regular Paper

A Secure Data Exchange System in Wireless Delay Tolerant Network Using Attribute-Based Encryption

Amang Sudarsono[1,a)] Toru Nakanishi[2,b)]

Received: June 7, 2016, Accepted: November 1, 2016

Abstract: Recently, Delay Tolerant Networks (DTNs) have been intensively researched to overcome unstable communication due to the intermittent link connection in wireless communications. In wireless DTNs, to enable continuous connectivity, data are exchanged through intermediate nodes in the path toward the destination node by store-and-forward approach. However, since the participating nodes in the network are not fully trusted, a secure data exchange mechanism in the DTNs would be strongly desirable. In this paper, we propose a secure data exchange system in the wireless DTNs using Attribute-Based Encryption (ABE) to provide two properties: (i) content data can be accessed by only authorized nodes that are dynamically defined by a policy on the attributes while keeping its integrity from alteration during transmission, and (ii) routing messages are encrypted and authenticated such that only the attribute-based authorized nodes can exchange the routing messages, where multi-hop routing messages are encrypted and authenticated by the ABE. Our experimental results show the practicality of our system.

Keywords: DTN, Attribute-Based Encryption, AES, MAC, flooding routing.

1. Introduction

As mobile devices with wireless connectivity are rapidly deployed, multi-hop wireless infrastructure-less networks have been paid attentions. The networks include Wireless Sensor Networks (WSNs) [7], Mobile Ad-hoc NETworks (MANETs) [20], Vehicle Ad-hoc NETworks (VANETs) [9], etc. In such networks, mobile devices construct their own autonomous network topology to communicate with each other, by exchanging routing messages to update their routing tables. The network topology may change either quickly or slowly, depending on the mobility of participating nodes, and moreover the mobile devices may join or leave to and from the network (e.g., moving away from the network and running out of the battery). This potentially causes an unstable link connection in the path from source node to destination node. DTNs (Delay Tolerant Networks) [21], [28], [29], [30] with routing consideration [3], [8], [9], [10], [18], [24], [25] to overcome the intermittent link connection have been intensively researched. In a DTN, the link between nodes with unstable connectivity can be established properly by store-and-forward approach [29]. In this approach, packets are stored in an intermediate node in the path toward the destination node while the link to the next node in the path is not available, and the packets are forwarded to the next node after the link becomes available. As example scenarios where the DTNs are applicable, the military operations [22] and the mobile environment [23] are considered. In the applications where content data are exchanged using the DTN, participating nodes store and forward the content data and exchange the routing messages. In DTNs, routing protocols are important to construct the autonomous networks, and thus the routing protocols such as flooding routing protocols and forwarding routing protocols have been comprehensively investigated, examined, and compared [18], [25] to improve the delay and performance for transferring data from source node to destination node.

However, in DTNs, the participating nodes are not fully trusted, and an adversary may participate in the network. Therefore, a security mechanism in DTNs for such non-trusted environments would be strongly desirable. To prevent unauthorized node's access to the content data exchanged among the nodes, we can apply some cryptosystems between end nodes, as follows. Before sending the data, the source node encrypts the data, which is forwarded and successfully decrypted only by the group of authorized destination nodes. In the access control, the flexibility and granularity of the access control is required, which depends on the adopted cryptosystem. The previous works [19], [20] employed Attribute-Based Encryption (ABE) [15] for encrypting the content data exchanged in DTNs. The access is controlled using the attribute possession of the nodes, where a secret key corresponding to each own attribute is issued securely during the initial registration phase. Encrypted original data can only be accessed by authorized nodes that are dynamically defined by a policy on the attributes. Thus, using ABE, we can achieve a flexible fine-grained access control based on the node's attributes. In Ref. [19], the authors proposed and implemented an access control scheme based on an ABE [15] in DTNs. They showed an example of the battlefield DTN scenario for several members of different ranks from US Army and Navy. Meanwhile, Ref. [20] described a flex-

[1] Department of Electrical Engineering, Electronics Engineering Polytechnic Institute of Surabaya (EEPIS), Surabaya, Indonesia
[2] Department of Information Engineering, Hiroshima University, Higashi-Hiroshima, Hiroshima 739–8511, Japan
[a)] amang@pens.ac.id
[b)] t-nakanishi@hiroshima-u.ac.jp

ible security solution in DTNs to let messages destined to representative names to be sent securely such that adversaries are not able to eavesdrop the messages easily. The solution implemented a prototype system using JAVA based RAPID router [17]. However, in the existing ABE-based schemes, only the confidentiality of the content data is addressed, but the security of routing messages is not considered. The routing message is very important information for all nodes in DTNs to update their routing tables in selecting the best path toward the destination node. Thus, the routing messages also should be hidden and authenticated.

In this paper [*1], we propose a secure data exchange system in the wireless DTNs, where the routing messages are hidden and authenticated using the ABE, in addition to the content data. Furthermore, we implement a prototype system with multi-hop routing, and show the experimental results to confirm the practicality. For the multi-hop routing, we adopt the flooding routing strategy [18], [25], concretely epidemic routing protocol [3] to construct an autonomous network topology: a node sprays its routing message to all neighbor nodes. Then, neighbor nodes relay the message to other adjacent nodes. In this strategy, it replicates the message to adequate nodes, where each node can update its routing table. Our motivation to employ the ABE in our system is to distribute the secret key used for a symmetric encryption and message authentication to the attribute-based authorized nodes so that the confidentiality and integrity of routing messages can be ensured.

In our system, a key distributor node firstly encrypts the symmetric key using the ABE and distributes it to all participating nodes together with the node's signature on the encrypted symmetric key and the certificate which includes the node's public key. The use of the digital signature and certificate is to guarantee that the transmitted encrypted symmetric key is originated from the key distributor node and not altered during transmission. Only the nodes that match a particular attribute policy are able to extract the key after verifying the key distributor node's signature. Then, the routing message is encrypted and authenticated by AES and MAC using the shared symmetric key. Thus, only the authorized participating nodes (indicated by the ABE) are able to exchange routing messages to construct a secure network topology. In addition, after establishing the best path between source node and destination node, by using the authenticated ABE for another particular attribute policy, the content data is encrypted using hybrid approach, whereas content data is encrypted using AES with temporary symmetric key. The temporary key for AES is encrypted using ABE, where the resulting ciphertext is sent together with encrypted content data and the signature of the ciphertexts with the certificate, and then they are exchanged to the authorized nodes. In our implementation, we employ a data access authorization for the network administration of IT department structure in our attribute policy scenario.

2. Security Requirements of Proposed Data Exchange System in Wireless DTNs

Tselikis et al. [4] identified security requirements in the DTN at the bundle level. In the DTN, the bundle is a packet containing important data exchanged hop by hop through the bundle protocol. Bundles are routed in a store-and-forward mechanism between nodes over the bundle layer through the bundle protocol.

Participating nodes in the wireless DTN, which receive, store, and forward data as the intermediate node, can easily access and read the bundles. Meanwhile, everyone including an adversary has a possibility to join the wireless DTN without any permission from a network administrator. Then, the adversary can illegally transmit bad data, or intercept the important data, modify, and retransmit it. In such situation, the most serious threats are against the content data exchanged among the nodes. The adversary joining the wireless DTN may access the content data in the bundle that is stored and forwarded hop by hop. The content data must be read by only the authorized target nodes, and the integrity must be ensured.

In addition to the security for content data, our motivation for the security consideration in the wireless DTN is to address the vulnerability of the routing protocol in wireless DTNs. Another one of important data exchanged among participating nodes is the routing message. When the nodes act as intermediate nodes, they are able to receive and re-advertise the routing messages from and to neighbor nodes in constructing and renovating an autonomous wireless DTN with the store-and-forward feature. Then, an adversary who acts as the relay node can confuse the routing in the autonomous network by distributing fake routing messages to other nodes. As a result, the adversary may stop routing messages to specific nodes. Since routing messages are potentially broadcasted to all neighbor nodes, the adversary may cause a traffic congestion of routing messages due to redundant routing messages distribution. Therefore, to protect the adversary's poisoning the routing messages, we require the integrity of the routing messages.

On the other hand, routing messages can potentially reveal the sensitive routing information that is useful for outside adversaries. For example, the network topology may provide the adversaries with the important information of attacking points and holes for network attacks such as Denial of Service (DOS). Thus, we also require the confidentiality of the routing messages.

Based on the above consideration, we define the security requirements in the proposed system over wireless DTN as follows:

- *Security of routing protocol.*
  - **Confidentiality of routing messages**: No node except authorized nodes is able to fetch the routing messages exchanged among the authorized nodes.
  - **Integrity of routing messages**: Only authorized nodes are able to participate in the routing mechanism, receive, and re-advertise the routing messages to other nodes. In other words, routing messages should be authenticated to guarantee that routing messages are derived from only authorized nodes and not modified during propagation.
- *Security of content data.*
  - **Confidentiality of content data**: No node except the authorized nodes is able to fetch the original content data.
  - **Integrity of content data**: The exchanged content data should be authenticated to guarantee that the content data

[*1] The preliminary versions of this paper were presented in Refs. [13], [14].

are not modified by non-authorized nodes during the store-and-forward mechanism.

3. Adopted Cryptographic Primitives

In this section, we review the ABE scheme [15], the symmetric encryption and message authentication, and digital signature, which are adopted in our proposed secure data exchange system in wireless DTN.

3.1 Attribute Based-Encryption Scheme

Bethencourt et al. [15] proposed the concept of a Ciphertext Policy Attribute-Based Encryption (CP-ABE) scheme, as a type of ABE. In this scheme, a message M is encrypted with an access policy of attributes. The access policy is expressed by a logical relation on attributes. When a user, i.e., a node in the DTN setting, owns a set of attributes, the node is initially issued the secret key that is assigned to each own attribute from a trusted authority (Key Generator Server). Then, the encrypted M is decrypted based on the matching of the access policy and the node's attributes. Only the nodes who have a match to the policy are able to successfully extract the original M. Thus, using CP-ABE, the flexible fine-grained access control based on user's attributes can be achieved. In this scheme, there are three players involved in the system (as shown in **Fig. 1**) and four algorithms as follows:

- **Setup**: This algorithm is performed by a Key Generator Server. On given a security parameter, this algorithm randomly generates the public parameters PK and a master key MK. PK will be used for encryption and decryption mechanisms, meanwhile MK is used for generating nodes' secret keys.
- **KeyGen**: This algorithm is executed by Key Generator Server. On given a set of attributes S_i of node i, public parameter PK, and the master key MK, it randomly generates the node's secret key SK_i that associates with S_i.
- **Encryption**: This algorithm is operated by all participating nodes including routers that will act as encryptor. On given message M, an access policy of attributes T, and the public parameters PK, it randomly computes a ciphertext CT.
- **Decryption**: This algorithm is operated by all participating nodes that will act as decryptor. The inputs of algorithm are public parameter PK, ciphertext CT, and a secret key SK_i bound to a set of attributes S_i. If and only if S_i satisfies the attribute policy T associated with CT, it is able to recover the original message M.

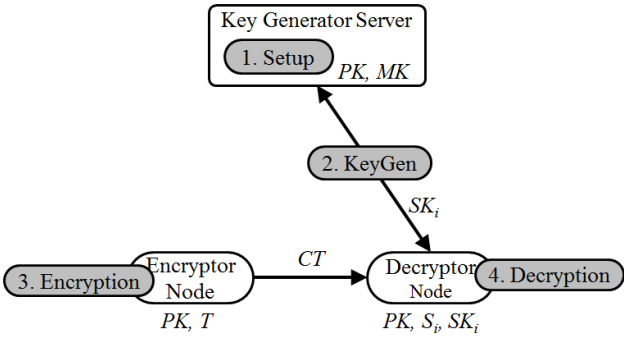

Fig. 1 Involved players and algorithms in CP-ABE.

Table 1 shows an example of attributes and the values. Let consider an example that a user i has a set of attributes, S_i = ("Male," "Lecturer," "A University," "Information Tech.," "3rd fl A Building"). On given a ciphertext with an access policy of attributes, T = ("Dean" $\vee$ ("Lecturer" $\wedge$ "Information Tech.")), then user i has the attributes satisfying the policy structure and thus can decrypt the ciphertext. However, if T = ("Dean" $\vee$ ("Staff" $\wedge$ "Information Tech.")), user i's attributes do not satisfy the policy, and hence user i cannot decrypt the ciphertext.

As another type of ABE, a Key-Policy ABE (KP-ABE) scheme has been proposed [16]. In KP-ABE, the user's secret key is generated from the access policy, and the ciphertext is correspondent to attributes, where only the user with the policy satisfied by the ciphertext's attributes can decrypt the ciphertext. For the scenario of the wireless DTN considered in this paper, the CP-ABE is used, and the KP-ABE is not used. Although any CP-ABE scheme can be adopted, the CP-ABE middleware of the scheme [15] is utilized in our implementation.

3.2 Symmetric Encryption and Message Authentication

For the fastness of encryption and message authentication, we adopt the hybrid approach: A symmetric key is encrypted by the CP-ABE. Using the shared symmetric key, the content data and routing messages are encrypted and authenticated.

For the symmetric encryption, we can utilize AES [1], where an encryptor encrypts data with any size using the shared symmetric key and the corresponding decryptor can decrypt the ciphertext using the same key. As the symmetric message authentication, MAC (Message Authentication Code) is used for checking the integrity of messages sent between the ends sharing the key. We utilize HMAC as the concrete instance of MAC.

For the authenticated encryption using the symmetric key, there are 3 approaches: (1) Encrypt-then-MAC (EtM) which firstly message is encrypted, then a MAC is created based on the encrypted message, (2) Encrypt-and-MAC (E&M) which firstly a MAC is created on message, then the message is encrypted without MAC, and (3) MAC-then-Encrypt (MtE) which firstly a MAC is created on message, then the message and its MAC are together encrypted. Among them, EtM approach provides the highest security in authenticated encryption when the used MAC is strongly unforgeable [2], [11], and becomes a standard method to ISO/IEC [12]. Thus, we adopt EtM approach in routing message.

3.3 Digital Signature

We adopt an RSA-based digital signature and the public key

Table 1 Example of attributes and the values.

Attributes	Example values
1) gender	Male, Female, ...
2) occupation	Lecturer, Doctor, Policeman, ...
3) academic degree	B.S, M.S, M.Sc, Dr, Ph.D, ...
4) major	Engineering, Science, Economic, ...
5) affiliation	A University, B College, C Institute, ...
6) faculty	Business, Engineering, Medical, ...
7) department	Information Tech., Multimedia, ...
8) division	Electrical, Industrial Tech., ...
9) position	Director, President, Dean, Staff, ...
10) location	1st fl D3 Building, 3rd fl A Building, ...

certificate in X.509 standard format [1], to guarantee the legitimacy of source nodes and to prevent the alteration of the encrypted keys.

4. Routing Protocols in DTN

In DTN, the exchange of routing messages also follows the store-and-forward mechanism. The nodes have the capability to store incoming routing messages in the buffer. When the routing message is exchanged between two or more nodes in the transmission range of each other, the nodes deliver them to the other relay nodes toward destination node [8], [18], [25]. In the mobile ad-hoc network, to deliver data from a source node to a destination node, firstly the setup phase is performed to determine a path from the source node to the destination node. Secondly, the data transmission and the maintenance of routing messages are done until the transmission is over. In DTN, the strategy of routing protocols is mainly comprised into two strategies: *flooding* family of routing protocols that replicate the routing messages to adequate nodes toward the destination node, and *forwarding* family of routing protocols that utilize the knowledge about the network status to determine the best path toward the destination node.

- **Flooding family**: In the flooding routing protocol, the replicas of same routing messages will be delivered to relay nodes toward the destination node. No knowledge about the network status among nodes is needed to operate this protocol. This routing protocol has some advantages: (i) high probability for successful messages delivery, and (ii) high probability to link the source node with the destination node in the transmission range.
- **Forwarding family**: The knowledge about network status including network topology is required in order to find the best path from the source node to the destination node. The difference from the flooding routing protocol is that this protocol does not need any message replication, but parameters regarding the network have to be exchanged to estimate each path. This protocol has the advantages: (i) the network resources including bandwidth, storage and energy are not wasted, (ii) the network congestion does not happen, and (iii) the network is scalable.

5. Proposed Secure Data Exchange System Using ABE

In this section, we describe our proposed system construction of a secure data exchange system using ABE in a wireless DTN.

5.1 Overview of System Construction

The proposed system mainly utilizes the CP-ABE scheme [15]. In the similar way to the previous works [19], [20], the exchanged content data are encrypted using the CP-ABE, and the ciphertext is sent from the source node to the destination node in the store-and-forward way of the DTN. Due to the hybrid approach, the temporal key is encrypted by CP-ABE, and the content data is encrypted by AES on the key. To ensure the legitimacy of the content data, a digital signature with the certificate is employed.

In addition, the routing messages are also encrypted and authenticated using the CP-ABE, as follows. A symmetric key encrypted by the CP-ABE is distributed from a representative routing node to all participating nodes with attributes showing the routing privilege, where the encrypted key is also authenticated by the digital signature. An advertiser node encrypts the routing message using AES, to which the MAC authenticating the encrypted message is appended. This is why only authorized routing nodes can update their routing tables. Our proposed system architecture is described in **Fig. 2**.

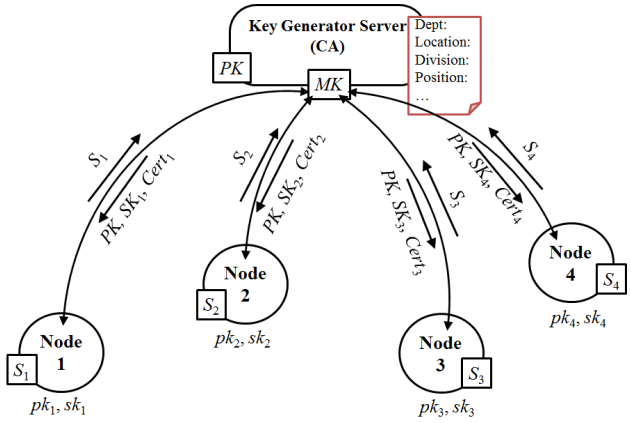

Fig. 2 System architecture of key generation phase.

5.2 Our Approach of Secure Data Exchange in Multi-hop Routing

In this paper, we consider wireless DTNs, where mobile devices may move quickly or slowly, join to the network, move away from the network, or run out of the battery. In addition, we consider sparse networks, where the connection of devices is intermittent, but the congestion of communication is rare. The store-and-forward mechanism in DTNs enables the stable communication in the networks. In such a setting, the flooding family of routing protocols is better than the forwarding family, since the higher deliver probability is expected, while the congestion due to lots of replications does not happen.

In the surveys about routing protocols in DTN [18], [25], there are some flooding routing strategies such as direct contact, two-hop relay, tree-based flooding, epidemic routing, prioritized epidemic routing, and probabilistic routing. Among them, we adopt the epidemic routing [3] of flooding family. Epidemic routing is flooding-based in nature, where every node continuously replicates and transmits routing messages to adjacent nodes including newly joining nodes that have not yet possessed a copy of the routing message. Generally, this protocol is used in the most simple case, since epidemic routing causes only flooding of routing messages. Because of this simplicity, the security mechanism based on CP-ABE can be more easily integrated. In addition, the epidemic routing protocol has the multiple-hop count needed for multi-hop routing, supports routing based on a routing table, and achieves the low latency.

In our construction of multi-hop data exchange in DTN, we divide the system into four phases: key generation phase, symmetric key distribution phase, path establishment phase, and content data transfer phase. In our proposed system, the path establishment phase is separated from the symmetric key distribution

phase. For the path establishment phase, the symmetric key distribution phase has to be executed once beforehand. In a fixed interval, each node can exchange its routing message encrypted using the same symmetric key to relay nodes, where the time-consuming CP-ABE encryption/decryption are not needed.

5.3 Construction of Proposed System

In the construction and implementation, we assume a simple multi-hop scenario, where four mobile nodes (Node 1 to Node 4) participate and each node sequentially communicates to the successive node in turn. We consider that our construction in this setting can represent the essentials of wireless DTN with the above-mentioned security. This is because the performance of routing process and transmission process in the secure wireless DTN can be demonstrated and measured in participants of sender node, relay nodes, and a receiver node. Furthermore, in this setting of two relay nodes, we can demonstrate a 2-hop communication scenario including the situations of a relay node's leaving or re-joining. The implementation and measurements for the more realistic settings with more nodes and non-sequential communications are our future works.

Each phase of our proposed system is as follows.

5.3.1 Key Generation Phase

This phase is initially executed out of wireless DTN and conducted by Key Generator Server (KGS). Here, we assume that KGS also acts as a Certificate Authority (CA). Every joining node i has already been generated a key pair, i.e., secret key sk_i and public key pk_i, and CA has issued the public key certificate $Cert_i$ to joining node i. In addition, we assume that every node owns the public key of CA to verify the certificate. Moreover, KGS issues a secret key that corresponds attributes of each node. This phase is illustrated in Fig. 2. We adopt the Setup and KeyGen algorithms of CP-ABE scheme [15]. Firstly, KGS generates public key parameters PK and master key MK. KGS obtains and confirms the set of attributes of each joining nodes (i.e., Node 1 to Node 4). Let assume S_i be a set of attributes of Node i. On supplied (MK, S_i), KGS creates a secret key SK_i that associates with S_i, and returns SK_i along with PK to the joining Node i.

We adopt the scenario in some IT departments of a campus, and each node has attributes of the building of the room, department name, position, etc. Moreover, we assume that some nodes have attributes of developers or administrators. These could be the routing-initiator nodes when starting to flood routing messages to their adjacent nodes.

5.3.2 Symmetric Key Distribution Phase

This phase has a goal to distribute a symmetric key K to all participating nodes. The symmetric key K consists of two key elements, K_{AES} and K_{HMAC}, where K_{AES} is a key for AES and K_{HMAC} is a key for HMAC authentication. These keys will be used for encrypting and authenticating routing messages exchanged among all participating nodes. The routing message will be encrypted by AES using symmetric key K_{AES} along with its MAC and sent to all relay nodes, in the following path establishment phase. In our scenario, we choose the routing-initiator node as a symmetric key generator node. Let assume that Node 1 is the symmetric key generator node. The protocol is shown in **Fig. 3**.

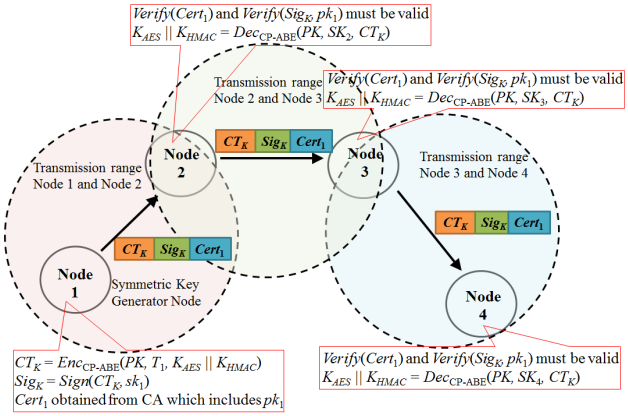

Fig. 3 Proposed protocol of symmetric key distribution phase.

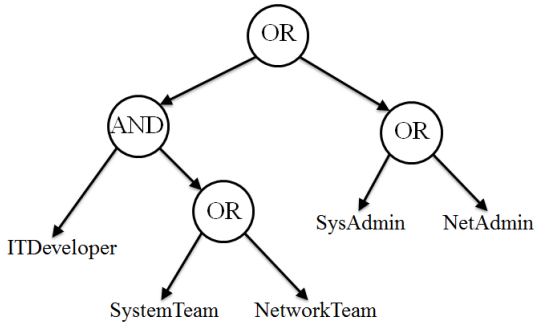

Fig. 4 Access policy of attributes T_1 for routing message exchange.

The symmetric keys K_{AES} and K_{HMAC} are 128-bit randomly selected by the symmetric key generator node. Then, they are encrypted by the CP-ABE with the attribute policy showing the routing privilege, and distributed from the symmetric key generator node to all participating nodes (i.e., Node 2, Node 3, and Node 4). Namely, the symmetric key generator node creates a ciphertext $CT_K = Enc_{CP-ABE}(PK, T_1, K_{AES} \| K_{HMAC})$, where Enc_{CP-ABE} is the CP-ABE Encryption algorithm, and T_1 is the access policy of attributes. In our scenario, we consider an example of the policy in **Fig. 4**, which can be represented as:

$$T_1 = (\text{“ITDeveloper”} \wedge (\text{“SystemTeam”} \vee \text{“NetworkTeam”})) \vee (\text{“SysAdmin”} \vee \text{“NetAdmin”}).$$

To ensure that CT_K is really distributed from a legitimated key generator node, i.e., to prevent CT_K from being modified during the transmission, Node 1 signs CT_K using its secret key sk_1, as $Sig_K = Sign(CT_K, sk_1)$, where $Sign$ is the signing function. Then, Node 1 distributes CT_K together with Sig_K and its certificate obtained from the CA, $Cert_1$ which carries its public key pk_1.

Upon receiving CT_K, Sig_K, and $Cert_1$, every authorized node firstly verifies $Cert_1$. If and only if $Cert_1$ is valid, then the node extracts Node 1's public key pk_1 from $Cert_1$. Furthermore, the extracted pk_1 is used for verifying Sig_K, by the verifying function $Verify(Sig_K, pk_1)$. If and only if the verification is valid, then the node decrypts CT_K to obtain the symmetric keys K_{AES} and K_{HMAC} by CP-ABE decryption algorithm $Dec_{CP-ABE}(PK, SK_i, CT_K)$ using node's secret key SK_i. Assuming that the nodes own the attributes of the developer or admin such as “SysAdmin,” then the nodes can decrypt the CT_K, since

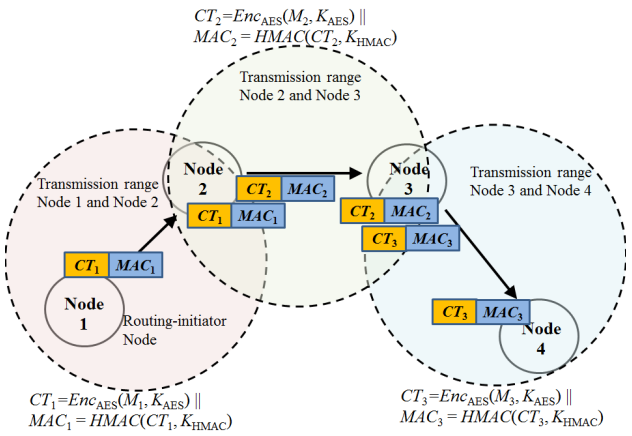

Fig. 5 Proposed protocol of path establishment phase.

the attribute fulfills the access policy T_1. Hence, only the nodes with the attribute matching to access policy T_1 are able to obtain valid K_{AES} and K_{HMAC} that are distributed from the symmetric key generator node. On the other hand, unauthorized nodes including adversaries are not able to recover the valid K_{AES} and K_{HMAC}.

The distribution process in the symmetric key distribution phase is also illustrated in Fig. 3. To distribute the symmetric keys K_{AES} and K_{HMAC} from Node 1 as the symmetric key generator node to Node 2, Node 3, and Node 4, we employ the same distribution process as the epidemic routing protocol over a DTN which enables store-and-forward approach. Firstly, Node 1 sprays CT_K, Sig_K, and $Cert_1$ to participating nodes in its transmission range over DTN. If no participating node in the transmission range, CT_K, Sig_K, and $Cert_1$ are stored and then whenever nodes exist in its transmission range, CT_K, Sig_K, and $Cert_1$ are forwarded to the nodes. Let assume Node 2 is in the transmission range of Node 1, thus CT_K, Sig_K, and $Cert_1$ are sprayed to Node 2. Upon receiving CT_K, Sig_K, and $Cert_1$, after verifying $Cert_1$ and Sig_K, by using its secret key SK_2, Node 2 decrypts CT_K to obtain K_{AES} and K_{HMAC}. Then, Node 2 forwards CT_K, Sig_K, and $Cert_1$ to other nodes in its transmission range. Let assume Node 3 is in the transmission range of Node 2, then Node 3 receives CT_K, Sig_K, and $Cert_1$, verifies $Cert_1$and Sig_K, and decrypts CT_K to get K_{AES} and K_{HMAC}. This process is continued from the sprayed nodes to the neighbor nodes in turn (e.g., from Node 3 to Node 4).

5.3.3 Path Establishment Phase

Using K_{AES} and K_{HMAC} obtained in the symmetric key distribution phase, a routing-initiator node starts to encrypt the routing message using AES, whereas the MAC authenticating the encrypted routing message is appended. The protocol is shown in **Fig. 5**. Assume that Node 1 is a routing-initiator node. Firstly, Node 1 computes a ciphertext $CT_1 = Enc_{AES}(M_1, K_{AES})$ on routing message M_1 and then generates a MAC on CT_1 using K_{HMAC}, $MAC_1 = HMAC(CT_1, K_{HMAC})$, where Enc_{AES} is AES Encryption. Furthermore, Node 1 sprays CT_1 together with its MAC, $CT_1 \| MAC_1$ to all relay nodes. Assume that Node 2 is in the transmission range with Node 1. Then, Node 2 decrypts CT_1 to obtain M_1 received from Node 1 if and only if the received CT_1 is valid by comparing the received MAC_1 and its computed MAC

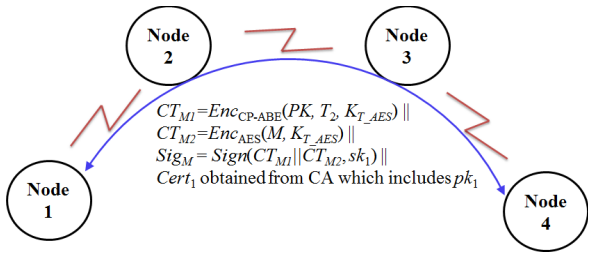

Fig. 6 Proposed protocol of content data transfer phase.

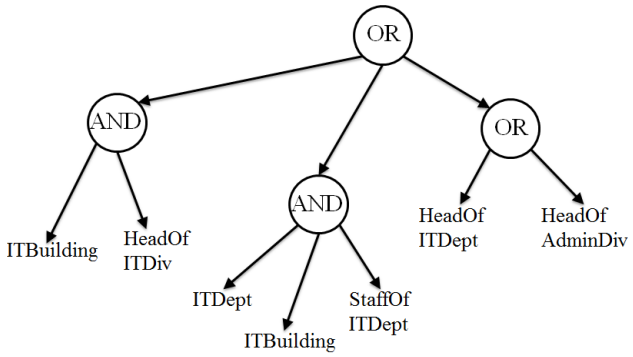

Fig. 7 Access policy of attributes T_2 for data transfer.

using its symmetric key K_{HMAC}, $MAC'_1 = HMAC(CT_1, K_{HMAC})$. Then, Node 2 updates its routing table based on the routing message M_1 from Node 1. In the similar way, Node 2 (resp., Node3) securely transmits its routing message M_2 (resp, M_3) to Node 3 (resp., Node 4) in turn. In a fixed interval, each node can exchange its encrypted routing message along with the MAC of encrypted routing message to relay nodes using the same symmetric key.

When the relay nodes are not in the transmission range with the advertiser node due to their mobility, running out the battery or other cases, the advertiser node stores the ciphertext and its MAC. When a relay node appears in the transmission range, the advertiser node forwards the data to the relay node.

5.3.4 Content Data Transfer Phase

Figure 6 illustrates the data transfer mechanism. This phase is executed by the nodes in the path from a source node to the destination node in the wireless DTN, after the path is established. Assume that Node 1 wants to share its resources (e.g., message, text, image, photo, or video files) to Node 4 in Fig. 6. As an example of the access policy, we consider T_2 in **Fig. 7**, which is represented as:

T_2 = (“ITBuilding” ∧ “HeadOfITDiv”)
∨ (“ITDept” ∧ “ITBuilding” ∧ “StaffOfITDept”)
∨ (“HeadOfITDept” ∨ “HeadOfAdminDiv”).

Assume that Node 4 owns the attributes satisfying T_2 such as “HeadOfITDept.” Firstly, Node 1 selects randomly a 128-bit temporary key K_{T_AES} and encrypts the key using the access policy T_2 as $CT_{M1} = Enc_{CP\text{-}ABE}(PK, T_2, K_{T\_AES})$. Then, Node 1 encrypts the content data M using AES encryption with K_{T_AES}, $CT_{M2} = Enc_{AES}(M, K_{T\_AES})$. For the ciphertexts, $CT_M = CT_{M1} \| CT_{M2}$, Node 1 signs CT_M using its secret key sk_1, $Sig_M = Sign(CT_M, sk_1)$. CT_M, Sig_M, and $Cert_1$ are sent together to Node 4 via the established path using the DTN mechanism of

the store-and-forward method. Note that for every content data exchange, the source node freshly generates 128-bit temporary key, K_{T_AES}.

Upon receiving the encrypted content data CT_M, Sig_M, and $Cert_1$ from Node 1, firstly Node 4 verifies $Cert_1$, if and only if $Cert_1$ is valid, Node 4 extracts pk_1 from $Cert_1$ and verifies Sig_M using pk_1, by $Verify(Sig_M, pk_1)$. If and only if the verification is valid, Node 4 decrypts CT_{M1} by using its secret key SK_4 corresponding the attributes satisfying the policy T_2, $K_{T\_AES} = Dec_{CP-ABE}(PK, SK_4, CT_{M1})$, and successfully fetches the valid temporary key for AES decryption, K_{T_AES}. Then, Node 4 decrypts CT_{M2} using AES decryption with K_{T_AES}, $M = Dec_{AES}(CT_{M2}, K_{T\_AES})$.

5.4 Security Discussion

Here, we discuss that the proposed system meets the security requirements defined in Section 2.

5.4.1 Security of Routing Protocol

When nodes act as the relay nodes, they receive and redistribute the routing messages from and to their adjacent nodes in establishing and maintaining a wireless DTN topology through store-and-forward mechanism. Here, we introduced two 128-bit symmetric keys K_{AES} and K_{HMAC}. In the symmetric key distribution phase, the keys are encrypted by CP-ABE related to the attribute policy T_1 and distributed. Unauthorized nodes that do not possess attributes satisfying the attribute policy T_1 cannot decrypt the ciphertext to obtain the keys. The CP-ABE ciphertext CT_K for the symmetric keys is signed by the symmetric key generator node (Node 1), and the signature Sig_K and the public key certificate $Cert_1$ are distributed and verified by other nodes. Thus, it is ensured that CT_K and the keys are generated by the authorized originator (Node 1) and not modified by non-authorized nodes. Therefore, only authorized nodes can share the symmetric keys. On the other hand, the routing message of Node i, M_i is encrypted by AES using K_{AES} in the path establishment phase. Thus, routing messages are kept secret to unauthorized nodes, including adversary nodes. This is why the confidentiality of routing messages holds.

Similarly, in the path establishment phase, the symmetric key K_{HMAC} shared among the authorized nodes is used for authenticating M_i through MAC to guarantee the originality of M_i. Thus, the routing messages from only the authorized nodes with the key K_{HMAC} can be accepted as valid routing messages in the routing protocol. Thus, unauthorized nodes including adversary nodes are not able to distribute fake routing messages. This is why the integrity of routing messages holds.

5.4.2 Security of Content Data

The temporal key K_{T_AES} is encrypted by CP-ABE related to the attribute policy T_2. Thus, only the authorized nodes are able to extract the temporal key. Furthermore, K_{T_AES} is used for encrypting M. Hence, the content data are hidden for the non-authorized nodes. In addition, the ciphertext of key and ciphertext of M are signed, and the signature and the certificate are sent and verified by the receiver. Thus, it is ensured that the data are originated from the legitimated sender node and not modified by the non-authorized nodes. Therefore, the confidentiality and integrity of content data hold.

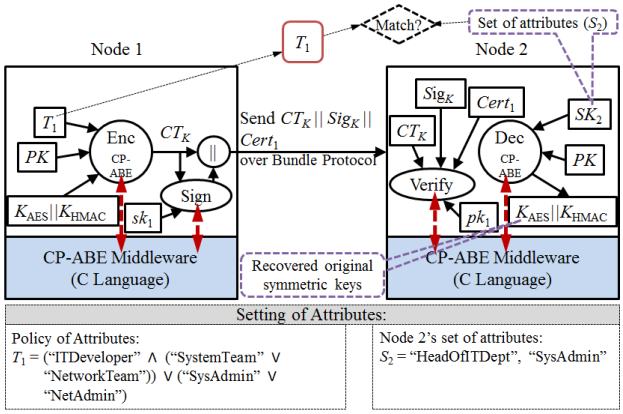

Fig. 8 Implementation of symmetric key distribution phase.

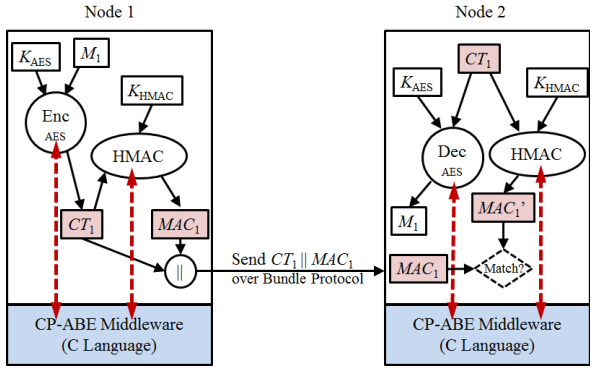

Fig. 9 Implementation of path establishment phase.

6. Implementation and Experimental Measurements

In this section, we describe our implementation of multi-hop routing data transfer using the CP-ABE and present the experiment results to show the effectiveness of the proposed system.

Our implementation was built on top of the underlying DTN system, which adopted DTN2 with standard protocols and architecture in Ref. [28]. Reference [28] is a reference of DTNRG: Delay Tolerant Networking Research Group which deals with request for comments (RFCs) standard on DTN architecture: RFC 4838 [29] and RFC 5050 [30]. The DTN2 system is implemented in C/C++ in supporting the multi-hop routing functionality. Furthermore, we also adopted a middleware [26] for the CP-ABE scheme [15], which is implemented on the PBC (Pairing-Based Cryptography) library [27] in C language. The PBC library is for the pairing and the underlying ECC computations used in the CP-ABE. We added the AES and HMAC algorithms into the middleware. For the AES and HMAC, we use the 128-bit symmetric keys. In addition, we incorporated 2048-bit RSA-based digital signature and the public key certificate of X.509 to our implementation using OpenSSL API Library [31]. **Figure 8**, **Fig. 9**, and **Fig. 10** illustrate the implementations for the main phases.

In Fig. 8 for the symmetric key distribution phase, Node 1 acts as a symmetric key generator node, selects K_{AES} and K_{HMAC}, and encrypts them by CP-ABE Encryption using PK and T_1, $CT_K = Enc_{CP-ABE}(PK, T_1, K_{AES}||K_{HMAC})$. In addition, Node 1

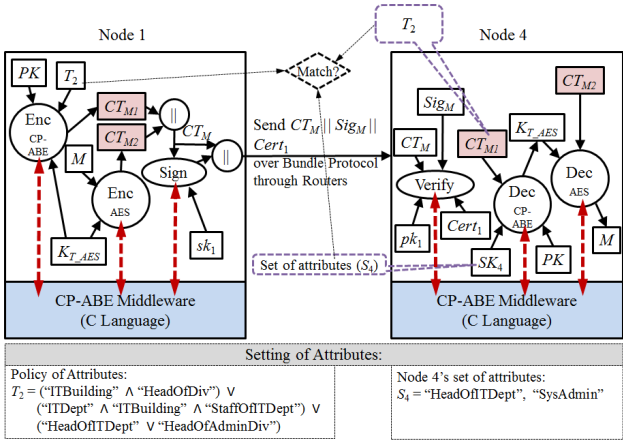

Fig. 10 Implementation of content data transfer phase.

Table 2 Specification of H/W (Node 1 to Node 4) used in experiment.

Software	gcc-4.4.5, gmp-5.1.1, pbc-lib-0.5.14, glib2.24, openssl-0.9.8o, oasys-1.6.0, dtn-2.9.0
O/S	Debian Linux kernel-2.6.32
CPU	Intel Core i7 1.80 GHz
RAM	2 GB
NIC	Intel Dual Band Wireless-N 7260, IEEE802.11a/b/g/n

signs CT_K using its sk_1, $Sig_K = Sign(CT_K, sk_1)$ and sends CT_K along with Sig_K and $Cert_1$. If and only if $Cert_1$ verification, extracting pk_1 and $Verify(Sig_K, pk_1)$ are valid, then if and only if Node 2's secret key SK_1 of the attributes matching policy T_1, Node 2 is able to decrypt and recover K_{AES} and K_{HMAC}. Figure 9 for the path establishment phase shows the use of K_{AES} and K_{HMAC} to encrypt and authenticate routing message M_1 in Node 1 acting as a routing-initiator node. Then, Node 1 sprays the encrypted message M_1, $CT_1 = Enc_{AES}(M_1, K_{AES})$ along with the MAC of C_1, $MAC_1 = HMAC(C_1, K_{HMAC})$ to Node 2. If and only if Node 2 has the same K_{AES} and K_{HMAC}, Node 2 is able to decrypt and authenticate M_1. Furthermore, Node 2 updates its routing table. Meanwhile, Fig. 10 for the content data transfer phase illustrates that Node 1 sends an encrypted content data M using CP-ABE encryption w.r.t. PK and T_2, $CT_M = CT_{M1}||CT_{M2}$, where $CT_{M1} = Enc_{CP-ABE}(PK, T_2, K_{T\_AES})$ and $CT_{M2} = Enc_{AES}(M, K_{T\_AES})$ together with the signature on CT_M, $Sig_M = Sign(CT_M, sk_1)$, and Node 1's certificate $Cert_1$. After verifying $cert_1$, extracting pk_1, and verifying Sig_M, if and only if Node 4 has the secret key SK_4 of the attributes matching policy T_2, Node 4 is able to decrypt and recover K_{T_AES}, and obtain M, by $M = Dec_{AES}(CT_{M2}, K_{T\_AES})$.

We measured the performance of our proposed system in laptop PCs. Our experiments topology consists of 4 laptop PCs acting as router nodes of DTN. Moreover, the specification of laptop PCs is shown in **Table 2**. Our measurements in three main phases of the implemented system are as follows.

6.1 Measurement for Symmetric Key Distribution Phase

The scenario of time measurement for symmetric key distribution is shown in **Fig. 11**. t_0 is the time of CP-ABE encryption of

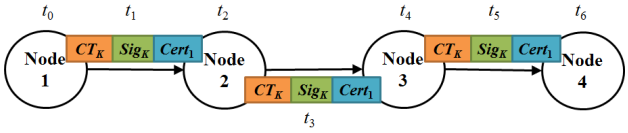

Fig. 11 Time measurement of symmetric key distribution.

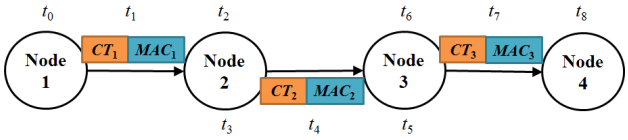

Fig. 12 Time measurement of 2-hop routing message exchange.

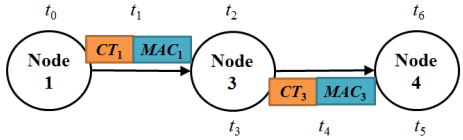

Fig. 13 Time measurement of routing message exchange after Node 2's leaving.

symmetric key K which consists of K_{AES} and K_{HMAC} and signing time on CT_K on Node 1. t_2, t_4, and t_6 are the time when CT_K together with Sig_K and $Cert_1$ are arrived, verification (which includes $Cert_1$ verification, pk_1 extraction from $Cert_1$, and Sig_K verification) is executed, and CT_K is decrypted (i.e., CP-ABE decryption computation), and then the recovered symmetric key is stored in Node 2, Node 3, and Node 4, respectively. t_1, t_3, and t_5 are communication time to propagate ciphertext CT_K together with Sig_K and $Cert_1$ through IEEE802.11n WiFi connection. The total process of symmetric key distribution takes about 2,726 ms, which is accumulation of t_0 to t_6. The time of CP-ABE encryption for $K_{AES}||K_{HMAC}$ on T_1 is about 169 ms, signing time on CT_K is about 43 ms, transmission time of CT_K together with Sig_K and $Cert_1$ in a link is about 679 ms, verification time is about 49 ms and CP-ABE decryption time for recovering $K_{AES}||K_{HMAC}$ is about 105 ms.

6.2 Measurement for Path Establishment Phase

We measured the processing times for updating the routing table. Upon receiving K, each node announces its routing information M_i to all nodes every 180 seconds. The scenario of time measurement for routing message exchange is shown in **Fig. 12**. Again, we assume that Node 1 is the routing-initiator node. t_0, t_3, and t_6 are AES encryption and HMAC generation time of routing messages M_1, M_2, and M_3 on Node 1, Node 2, and Node 3, respectively. These times are about 0.64 ms for AES encryption and 0.16 ms for HMAC computation. t_1, t_4, and t_7 are the communication times to propagate a couple of (CT_i, MAC_i) through IEEE802.11n WiFi connection, which are about 493 ms. Meanwhile, t_2, t_5, and t_8 are the times of AES decryption, HMAC generation and comparison, and updating routing table on Node 2, Node 3, and Node 4, respectively, which are 0.53 ms for AES decryption, 0.29 ms for HMAC generation and comparison. Thus, the total time of routing message exchange on 2-hop among 4 nodes is about 1,668 ms.

If the relay node Node 2 leaves the network, then a routing message exchange happens again, as shown in **Fig. 13**. In this sit-

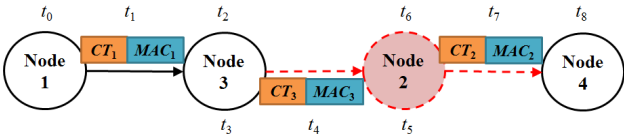

Fig. 14 Time measurement of routing message exchange after Node 2's re-joining.

Table 3 Processing times for exchanging various data.

Type of data (Original data size, encrypted data size, signature size, certificate size)	Encryption, signing, transmission, verification, decryption times (ms)	Total processing time (ms)
Text file (13 Bytes 2,485 Bytes 256 Bytes 1,330 Bytes)	210 43 2,043 48 101	2,672
Image file (176,813 Bytes 179,285 Bytes 256 Bytes 1,330 Bytes)	218 45 7,063 51 107	7,721
Image file (1,298,878 Bytes 1,301,349 Bytes 256 Bytes 1,330 Bytes)	246 56 40,201 51 141	41,086

uation, the total time for the routing message exchange is about 1,305 ms. **Figure 14** illustrates the situation where Node 2 re-joins to the network to construct the 2-hop routing message exchange. Here, all nodes reform the path from Node 1 to Node 4. This process requires the total time of 1,691 ms. Note that these times can exclude the time of the symmetric key distribution. From the results, the overhead of AES and HMAC is relatively small compared to the transmission time, and thus the proposed protocol is sufficiently practical.

6.3 Measurement for Content Data Transfer Phase

Table 3 shows the total times of transferring various types of data between Node 1 and Node 4 using CP-ABE based on access policy T_2. After establishing the path from Node 1 to Node 4, we transfer various data from Node 1 to Node 4, where Node 2 and Node 3 are the relay nodes. To exchange a text file with 13 Bytes, it totally takes about 2,672 ms, where the total encryption time is about 210 ms (197 ms for CP-ABE encryption and 0.54 ms for AES encryption), signing time is about 43 ms, the transmission time is about 2,043 ms, the total verification time is about 48 ms (22 ms for certificate verification, 3 ms for Node 1's public key extraction, and 21 ms for signature verification), and the total decryption time is about 101 ms (87 ms for CP-ABE decryption and 0.34 ms for AES decryption). To exchange the image file with 176,813 Bytes takes about 7,721 ms, where the encryption time is about 218 ms (198 ms for CP-ABE encryption and 6 ms for AES encryption), signing time is about 45 ms, the transmission time takes 7,063 ms, total verification time is about 51 ms (23 ms for certificate verification, 3 ms for Node 1's public key extraction from certificate, and 22 ms for signature verification), and the decryption time is about 107 ms (87 ms for CP-ABE decryption and 6 ms for AES decryption). For exchanging the image file with 1,298,878 Bytes, we need 41,086 ms. The encryption takes about 246 ms (199 ms for CP-ABE encryption and 44 ms for AES encryption) and the decryption time is 141 ms (88 ms for CP-ABE decryption and 38 ms for AES decryption). The signing time and total verification time are about 56 ms and 51 ms, respectively. The transmission time becomes 40,201 ms. From these results, the total exchanging time is dominated by the transmission time. Furthermore, while the transmission time increases as the exchanged content data is larger, the encryption time and decryption time are relatively stable. Therefore, we can confirm that the overhead of adopting the CP-ABE is relatively small and practical.

7. Conclusion

We have proposed a secure data exchange system with multi-hop routing in wireless DTNs using the Attribute-Based Encryption (ABE). The ABE scheme is utilized for encrypting and authenticating the routing message exchange, in addition to the authorization for the exchanged content data. The experimental results show the practicality of our system in the current environment of laptop PCs.

Our future works include the adoption of more efficient CP-ABE schemes with faster pairing-based library, and the implementation and evaluation of the proposed system in more participating nodes.

Acknowledgments This work was partially supported by Electric Technology Research Foundation of Chugoku.

References

[1] Stalling, W.: *Network Security Essentials: Applications and Standards (4th Edition)*, Pearson Education Inc., Prentice Hall (2011).
[2] Bellare, M. and Namprempre, C.: Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm, *Journal of Cryptology*, Vol.21, No.4, pp.469–491 (2008).
[3] Zhang, X., Neglia, G., Kurose, J. and Towsley, D.: Performance Modeling of Epidemic Routing, *Journal of Computer Networks, ScienceDirect*, pp.2867–2891 (2007).
[4] Tselikis, C., Poulakidas, A., Aggelis, A. and Ladis, E.G.: An Efficient Implementation of the Bundle Security Protocol for DTN-enabled Embedded Devices, *Journal of Applied Mathematics & Bioinformatics*, Vol.3, No.1, pp.163–170, ISSN: 1702-6602 (print), 1792-6939 (online), Scienpress Ltd. (2013).
[5] Chen, Y.S., Hsu, C.S. and Cheng, C.H.: Network Mobility Protocol for Vehicular Ad Hoc Networks, *Journal of Communication Systems*, Published online in Wiley InterScience, pp.1–35, DOI: 10.1002/dac (2010).
[6] Defrawy, K.E. and Tsudik, G.: ALARM: Anonymous Location-Aided Routing in Suspicious MANETs, *IEEE Transactions on Mobile Computing*, Vol.10, No.9, pp.1345–1358 (2011).
[7] Akyildiz, I.F., Su, W., Sankarasubramaniam, Y. and Cayirci, E.: Wireless Sensor Networks: A Survey, *Journal of Computer Networks*, Vol.38, No.4, pp.393–422 (2002).
[8] Gong, H. and Yu, L.: Study on routing protocols for delay tolerant mobile networks, *Journal of Distributed Sensor Networks*, Vol.2013, 16 pages, Hindawi Publishing Corporation (2013).
[9] Benamar, N., Singh, K.D., Benamar, M., Ouadghiri, D.E. and Bonnin, J.M.: Routing protocols in Vehicular Delay Tolerant Networks: A comprehensive survey, *Elsevier Journal on Computer Communications*, Vol.48, pp.141–158 (2014).
[10] Jones, E.P.C., Li, L., Schmidtke, J.K. and Ward, P.A.S.: Practical Routing in Delay-Tolerant Networks, *IEEE Transactions on Mobile Computing*, Vol.6, No.8, pp.943–959 (2007).
[11] Krawczyk, H.: The Order of Encryption and Authentication for Protecting Communications (or: How Secure Is SSL?), *Proc. 21st Annual International Cryptology Conference on Advances in Cryptology - CRYPTO'01*, pp.310–331 (2001).

[12] Information technology – Security techniques – Authenticated encryption, 19772:2009, ISO/IEC (2009).
[13] Sudarsono, A. and Nakanishi, T.: An Implementation of Secure Data Exchange in Wireless Delay Tolerant Network Using Attribute-Based Encryption, *CANDAR-WICS2014*, pp.536–542 (2014).
[14] Sudarsono, A. and Nakanishi, T.: An Implementation of Secure Data Exchange System with Multi-hop Routing in Wireless Delay Tolerant Network Using Attribute-Based Encryption, *CANDAR-WICS2015*, pp.470–476 (2015).
[15] Bethencourt, J., Sahai, A. and Waters, B.: Ciphertext-Policy Attribute-Based Encryption, *IEEE Symposium on Security and Privacy*, pp.321–334 (2007).
[16] Goyal, V., Pandey, O., Sahai, A. and Waters, B.: Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data, *Proc. 13th ACM Conference on Computer and Communications Security* (*CCS'06*), pp.89–98 (2006).
[17] Balasubramanian, A., Levine, B.N. and Venkataramani, A.: DTN Routing as a Resource Allocation Problem, *Proc. 2007 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications* (*SIGCOMM'07*), pp.373–384 (2007).
[18] Shen, J., Moh, S. and Chung, I.: Routing Protocols in Delay Tolerant Networks: A Comparative Survey, *Proc. 23rd International Technical Conference on Circuits/Systems, Computers and Communications* (*ITC-CSCC 2008*), pp.1577–1580 (2008).
[19] Roy, S. and Chuah, M.: Secure Data Retrieval Based on Ciphertext Policy Attribute-Based Encryption (CP-ABE) System for the DTNs, Lehigh CSE Technical Report (2009).
[20] Chuah, M., Roy, S. and Stoev, I.: Secure Descriptive Message Dissemination in DTNs, *Proc. MobiOpp'10, 2nd International Workshop on Mobile Opportunistic Networking*, pp.79–85 (2010).
[21] Venkataraman, V., Acharya, H.B. and Shah, H.: Delay Tolerant Networking-A Tutorial, available from ⟨http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.187.8553⟩.
[22] Marshall, P.: DARPA progress towards affordable, dense, and content focused tactical edge networks, *Military Communications Conference* (*MILCOM 2008*), pp.1–7 (2008).
[23] Keranen, A., Pitkanen, M., Vuori, M. and Ott, J.: Effect of Non-Cooperative Nodes in Mobile DTNs, *Proc. IEEE WoWMoM Workshop on Automatic and Opportunistic Communication* (*AOC*), pp.1–7 (2011).
[24] Jain, S., Fall, K. and Rabin, R.: Routing in a delay tolerant network, *Proc. 2004 Conference on Applications, Technologies, Architectures, and Protocls for Computer Communications* (*SIGCOMM 2004*), pp.145–158 (2004).
[25] Mangrulkar, R.S. and Atique, M.: Routing protocol for Delay Tolerant Network: A survey and comparison, *IEEE International Conference on Communication Control and Computing Technologies* (*ICCCCT*), pp.210–215 (2010).
[26] Bethencourt, J., Sahai, A. and Waters, B.: cpabe toolkit in Advanced Crypto Software Collection, available from ⟨http://hms.isi.jhu.edu/acsc/cpabe/⟩.
[27] Lynn, B.: PBC (Pairing-Based Cryptography) library, available from ⟨http://crypto.stanford.edu/pbc/⟩.
[28] DTNRG.: Delay Tolerant Networking Research Group, available from ⟨http://www.dtnrg.org/⟩.
[29] IETF.RFC 4838.: DTN Architecture (2007), available from ⟨http://www.ietf.org/rfc/rfc4838.txt⟩.
[30] IETF.RFC 5050.: DTN Architecture (2007), available from ⟨http://www.ietf.org/rfc/rfc5050.txt⟩.
[31] OpenSSL.: Cryptography and SSL/TLS Toolkit, available from ⟨https://www.openssl.org/⟩.

Amang Sudarsono received his B.E. degree in electrical engineering, telecommunication and multimedia program from Sepuluh Nopember Institute of Technology, Indonesia, in 2001. He received his Ph.D. degree in communication network engineering from Okayama University, Japan, in 2011. From 1997 to 2002, he was with the Network Engineering Division, Metro Cellular Nusantara, Ltd., Indonesia. He joined the Department of Electrical Engineering, Division of Telecommunication Engineering at Electronics Engineering Polytechnic Institute of Surabaya, Indonesia, as a lecturer in 2002. His research interests include group signature and network securities.

Toru Nakanishi received his M.S. and Ph.D. degrees in information and computer sciences from Osaka University, Japan, in 1995 and 2000, respectively. He joined the Department of Information Technology at Okayama University, Japan, as a research associate in 1998, and moved to the Department of Communication Network Engineering in 2000, where he became an assistant professor and an associate professor in 2003 and 2006, respectively. In 2014, he moved to the Department of Information Engineering at Hiroshima University as a professor. His research interests include cryptography and information security. He is a member of IEICE.