EMITTER International Journal of Engineering Technology
Vol. 4, No. 1, June 2016
ISSN: 2443-1168

Secure Communication and Information Exchange using Authenticated Ciphertext Policy Attribute-Based Encryption in Mobile Ad-hoc Network

Samsul Huda, Amang Sudarsono, Tri Harsono

Study Program of Applied Master's Degree Information and Computer Engineering
Graduate Program of Engineering Technology
Politeknik Elektronika Negeri Surabaya(PENS), Surabaya, Indonesia.
PENS Campus, Jl. Raya ITS Sukolilo, Surabaya 60111.
E-mail: samsul@pasca.student.pens.ac.id, {amang,trison}@pens.ac.id

Abstract

MANETs are considered as suitable for commercial applications such as law enforcement, conference meeting, and sharing information in a student classroom and critical services such as military operations, disaster relief, and rescue operations. Meanwhile, in military operation especially in the battlefield in freely medium which naturally needs high mobility and flexibility. Thus, applying MANETs make these networks vulnerable to various types of attacks such aspacket eavesdropping, data disseminating, message replay, message modification, and especially privacy issue. In this paper, we propose a secure communication and information exchange in MANET with considering secure adhoc routing and secure information exchange. Regarding privacy issue or anonymity, we use a reliable asymmetric encryption which protecting user privacy by utilizing insensitive user attributes as user identity, CP-ABE (Ciphertext-Policy Attribute-Based Encryption) cryptographic scheme. We also design protocols to implement the proposed scheme for various battlefied scenarios in real evironment using embedded devices. Our experimental results showed that the additional of HMAC (Keyed-Hash Message Authentication Code) and AES (Advanced Encryption standard) schemes using processor 1.2GHz only take processing time about 4.452 ms, we can confirm that our approach by using CP-ABE with added HMAC and AES schemes make low overhead.

Keywords: MANET, Attribute-Based Encryption, Information Confidentiality and Integrity.

1. INTRODUCTION

Communication systems using mobile devices such as smartphones, laptops, and embedded devices have become an integral part in modern era. Recently, mobile devices have bundled with wireless card which may directly communicate with others like exchanging data or information, even without any constructed the fixed infrastructure or internet connection. This network is commonly known as an Ad-hoc Network. When it is formed by collection of mobile devices, it is called a MANETs (Mobile Ad-hoc Networks)[1][8][9]. In MANETs, mobile devices can reach any other mobile device which are outside their range through the intermediate nodes by multi-hop or multiple relaying system over a dynamic topology. Furthermore, the mobility, flexibility and scalability are also the advantages of MANETs.

Due to their characteristics, MANETs are considered as suitable for commercial applications such as law enforcement, conference meeting, and sharing information in a student classroom and critical services like military operations, disaster relief, and rescue operations[12]. The need for exchanging information in military operations is very important such as strategy or tactic commands from captain, ammunition status or health condition from all participants in the battlefield. Meanwhile, battlefield operationin freely medium which naturally needs high mobility and flexibility [14][16][17]. Thus, by applying MANETs make these networks vulnerable to various types of attacks. The attacks include packet eavesdropping, data disseminating, message replay, message modification, and denial of service[1][12].

Table 1. Security issues in mobile adhoc network [1]

Layer	Security issues	Attacks
Application layer	Detecting and preventing viruses, worms, malicious codes, and application abuses	Repudiation, data corruption
Transport layer	Authenticating and securing end-to-end communications through data encryption	Session hijacking, SYN flooding
Network layer	Protecting the adhoc routing and forwarding protocols	Wormhole, blackhole, byzantine, flooding, resource consumption, location disclosure
Link layer	Protecting the wireless MAC protocol and providing link-layer security support	Traffic analysis, monitoring, disruption MAC(802.11), WEP weakness
Physical layer	Preventing signal jamming denial-of-service attacks	Jamming, interceptions, eavesdropping

As mentioned in [1], The security goals for MANETs is to provide some security services, such asauthentication, confidentiality, integrity,access control, non-repudiation and availability. Each layer has a different attack vulnerability. Table 1 describes the security issues and various attacks in each layer.Used single security in a system will not fully protect from unauthorized data breaches. Therefore, the security solution should provide full protection in all layers, but the importance layer must be secure are network and application layers [1]. Many researchers have worked on securing mobile ad-hoc networks mainly focus onthe link layer [9][10] and network layer[12][13][16]. They fulfill different security requirements and prevent specific attacks. [9] developed a cross-layer security solution based on cooperation between routing and MAC layers using hash function SHA-1 and MD5 under OLSR routing protocol. However, they only addressed one of the attacks targeting neighbor discovery phase in OLSR. This attack is launched atrouting level by implementing a VLINK attack (Virtual Link) leading to establish false symmetric link between the targeted nodes connected via an asymmetric link. [8] proposed secure content delivery in CCMANET (Content Centric MANET) with end-to-end authentication mechanism using Yaksha system digital signature algorithm, the variant of the RSA public-key crypto system. However, the anonymity and control access features are not provided.

Anonymity should be one important part of the overall solution for truly secure mobile ad-hoc networks, especially in certain privacy-vital environments. For example, in a battlefield, we do not want only to ensure that adversaries are not able to disclose the contentof our communications (i.e., confidentiality) or disable the communications (i.e., availability and integrity), but also expect that the parties' identities in communications are anonymous from adversaries. Otherwise, adversaries may deduce important information about the location or the mobility model of communicating parties, which can be used to locate the target of their physical attacks at a later time.

Meanwhile, from a variety of possible attacks described in Table 1, sensitive information is the primary target, either by interception or data modification. Therefore, it is needed for restrictions on the right of access only to authorized users. Moreover, the distribution of data through internet network. So, keeping the confidentiality, authenticity and integrity of data is a fundamental security solution in MANET application layers. [18] proposed secure authentication scheme in device-to-device connection (D2D) in two scenarios with a secure initial key establishment using CP-ABE. Practically, they implemented the scheme in mobile multi-hop networks environment and also analyzed the system performance [19]. However, the performance of the proposed scheme in proposed scenarios has not been presented, they only presented the CP-ABE algorithm performance in mobile devices.

[15] proposed design of a new multi-tier adaptive military MANET security protocol using hybrid cryptography and signcryption. The proposed design offered three main protocols : cryptographic methods used in MANETs, hybrid key management protocols and structural organization of the military MANETs. The authors mentioned that they used the hybrid cryptography mechanisms and ECPVSS (Elliptic Curve Pintsov Vanstone Signature Scheme) that provided security and performance advantages when compared to some traditional cryptographic methods. However, the proposed scheme only fulfilled the confidentiality, integrity and

authentication features on the information sharing scheme. In fact, privacy is indispensable in military operations with high mobility and freely medium. Furthermore, access restrictions using access control mechanism is also required.

ABE (Attribute Based Encryption) [6] is a new approach for encrypted access control. It offers security and access control. CP-ABE (Ciphertext-Policy Attribute-Based Encryption) [3] is one of variant of ABE algorithm. CP-ABE is a reliable asymmetric encryption mechanism that provides features to hide the user personal data by utilizing insensitive user attributes as user identity. In CP-ABE, The recipient only can decrypt if and only if the attribute set of his private key matches with the specified policy in the ciphertext. CP-ABE is appropriate for most applications, like for data exchange over wireless medium[4], Secure content exchange in DTN (Delay Tolerant Network)[5][7]. However, the CP-ABE algorihm is not supported data integrity service.

In this paper, we extend our previous work [4], by proposing a secure data exchange over wireless medium using CP-ABE in the military case study. In this work, we consider for constructing a security system in MANETs for military operation with enabling secure adhoc routing at network layer and information exchange at application layer. In order to secure network layer, we utilize S-OLSR (Secure Optimized Link State Routing) with coverthe security requirements : the authenticity ofthe other node and the integrity of the routing packets. In military operations, not only ensure the routing protocol, but also the confidentiality of information and the privacy protection of the identities of the participating nodes. Hence, for securing the application layer we consider any security requirements : data integrity, data confidentiality, authentication, access control and user privacy. To provide it, we choose CP-ABE algorithm which has advantages in access control and privacy features. The proposed scheme providesdata integrity, data confidentiality, and authentication services simultaneously. Data integrity and authentication are obtained through an added HMACscheme in encryption and decryption phases, respectively [4]. Then, we have reviewed its method and found the weakness ofthe potential vulnerability hole. The message authentication code *MAC*, one of the component outputs from encryption phase is sent in plaintext form. Therefore, in this paper, we enhance the security level by combining with symmetric cryptography technique. Thus, the output information which would be delivered through wireless link to the destination in ciphertext mode. In addition, we also propose different scenarios in battlefield implementation along with four protocols for implementingthe proposed system.Then, we evaluate the implementation of the proposed scheme in the real environment with embedded devices represented as participants to show the effectiveness of our system.

The rest of this paper is organized as follows. In Section 2, we describe authenticated CP-ABE as our previous work. Then, in Section3, we explain our adopted cryptographic scheme to construct our security goals. In Section

4, we explain our security requirements of the proposed scheme. In Section 5, we explain the detail of our proposed secure information exchange in MANET along with scenarios and protocols for implementation. Then, in Section 6, we present the implementation of our proposed scheme, experimental results and analysis. Finally, in Section 7 we express the conclusion and future works.

2. PREVIOUS WORK

In this section, we review an Authenticated-CPABE algorithm was developed in our previous work[4]. It supported access control and anonymity features by utilizing in sensitive user attributes as user identity. It has four functions, include Setup, Key Generation, Encryption, and Decryption. The access policy structure is related to the set of user attributes which are embedded in the secret key user *SK*. The access policy that presented by any monotonic access tree is linked with encrypted data, even if over radio link medium which is not secret, the confidentiality of data cannot be revealed. Only when the set of attributes associated with the decryption key corresponding with the access policy, the user will be able to decrypt the ciphertext *CT* and get back the plaintext *M*. This work provided data integrity, data confidentiality, and authentication services simultaneously.

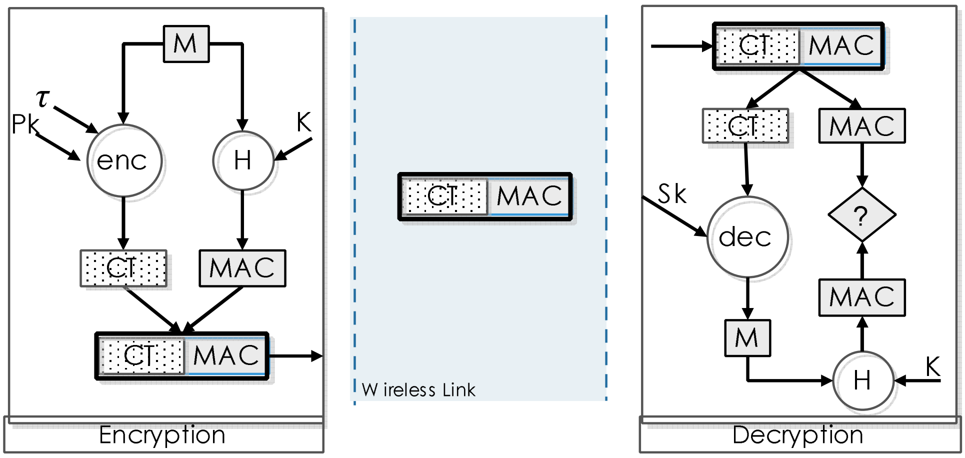

Figure 1. Authenticated CP-ABE construction [4]

The constructions of Authenticated-CP ABE consists of four phases includes setup, key generation,encryption and decryption. We adopt Setup and KeyGen algorithm from CP-ABE scheme [3]. The detail about this algorithm described in Figure 1.

Setup (*PK, MK*):On input a security parameter, this phase is performed within the user who acts to generate the public keys*PK* for all users and a master key *MK*, which is used for key generation and kept private. *PK* will be used for encryption and decryption mechanisms while *MK* will be functioned for generating user's secret keys *SK*. Firstly, we choose and let $\mathbb{G}_0$ be a bilinear group of prime order p, and let g be a generator of $\mathbb{G}_0$. In addition let a bilinear map e : e: $\mathbb{G}_0 \times \mathbb{G}_0 \rightarrow \mathbb{G}_1$.

$$PK = \mathbb{G}_{0,}g, h = g^{\beta}, f = g^{1/\beta}, e(g,g)^{\alpha} \quad (1)$$
$$MK = (\beta, g^{\alpha}) \quad (2)$$

KeyGen (*PK, MK, Att*):This phase actkey generation scheme. Key generation for a user requires two parameters, the *MK*, as well as *Att* the set of attributes that the user possesses. The attributes are insensitively. The output is a *SK* for the user. That's associated with *Att*. *SK* is generated by selecting a random $r \in Zp$and operated for each attribute of user.

$$SK = (D = g^{(\alpha+r)/\beta}, \forall j \in Att: D_j = g^{r}.H(j)^{r_j}, D'_j = g^{r_j}) \quad (3)$$

Encryption (*PK, M, τ, K*):This phase is run by all participating users who will act as an encryptor. Encryption algorithm encrypts a message *M* under an access policy *τ* which represents the attributes needed for decryption process. We utilize HMAC scheme with shared key *K* to enable authentication and data integrity service.So, data confidentiality, data integrity and authentication fulfilled simultaneously. It outputs a *CT* concatenate with *MAC* which are computed as:

$$CT = \begin{bmatrix} (\tau, \tilde{C} = M.e(g,g)^{\alpha Att}, C = h^{Att}, \\ \forall y \in Y: C_y = g^{q_y(0)}, C'_y = H(attr(y))^{q_y(0)}), \\ MAC = H(M,K) \end{bmatrix} \quad (4)$$

Decryption (*PK, CT, SK, K*):Decryption occurs when a user with personal key *SK* wishes to decrypt the ciphertext represented by *CT*. Decryption is the second step process, withthe first decrypting the message to determine if the ciphertext's access tree *τ*is satisfied by the user's properties within *SK*, and the second performing the verification of the message integrity *MAC*. This algorithm is operated by all participating users who act as a decryptor. On input a *CT*, a secret key *SK*. If and only if *Att* = *τ*and checking result of *MAC* is true. The message can be recovered to original message *M*, and error symbol ⊥ otherwise. It computed as :

$$Decrypt(CT,SK) = \begin{bmatrix} \frac{C_{x.}.A}{e(C2,D)} = \frac{C1.e(g,g)^{rAtt}}{e(h^{s}, g^{\alpha+r/\beta}} = \frac{M.e(g,g)^{\alpha Att}}{e(g,g)^{\alpha Att}}, \\ Verify(M,HMAC) = True/False \end{bmatrix} \quad (5)$$

3. ADOPTED CRYPTOGRAPHIC SCHEME

We adopt CP-ABE scheme [3], the symmetric encryption and message authentication [2] in our proposed secure information exchange in mobile ad-hoc network.

3.1 Ciphertext Policy Attribute-Based Encryption Scheme

In the CP-ABE scheme [3], a message M is encrypted using public key PK and an access policy that associated with attributes. The access policy is expressed by a logical relation on attributes. Each node has a set of attributes which expressed node's insensitively information like shown in Figure 2. The *SK*is issued by a trusted party,such as KGS (Key Generator Server). Then, the *CT* can be decrypted based on the matching of the access policy and the *SK*. Only the nodes who have attributes matched with the access policy are able to successfully decrypt and get back the original *M*. In the CP-ABE scheme, there are four algorithms as follows:

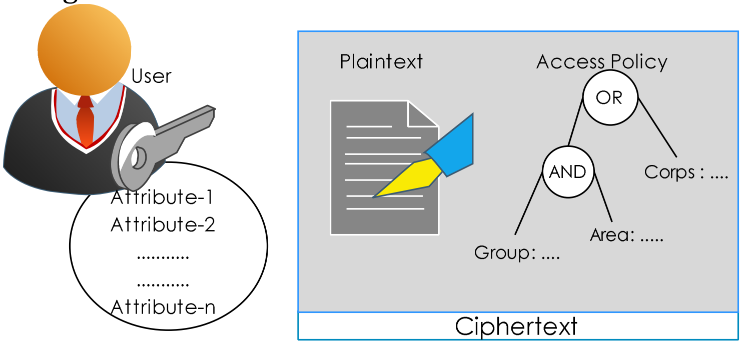

Figure 2. The fundamental of CP-ABE system [3]

Setup: On input a security parameter, this algorithm randomly outputs the *PK* and *MK* which is kept private. *PK* will be published for encryption and decryption mechanisms, while *MK* will be operated for generating user's secret keys *SK*.

KeyGen: On input the system *PK*, *MK* and attribute list of user*S*. User request *SK* to KGS by issued their attributes *S*. KGS executed this algorithm. It outputs a *SK* for user.

Encryption: On given message *M*, an access policy of attributes *T*, and the public parameters *PK*, it randomly computes a *CT*. This algorithm is performed by all participating users in the system who will act as an encryptor.

Decryption: On given *CT* and a secret key *SKi* bound to a set of attributes *Si*, user who has *Si* matching to the attribute policy *T* associated with *CT* is able to recover the original message *M*.

3.2 Symmetric Encryption and Message Authentication

As well as our previous work [3], For the fastness and strength of encryption and message integrity, we adopt the symmetric encryption and message authentication scheme [2]. HMAC is used for checking the integrity of the exchanged messages. We utilize HMAC as the concrete instance of *MAC*. We utilize AES-256 to enhancedata confidentiality and HMAC-SHA256 to satisfy the data integrity of the exchanged data.

4. SECURITY REQUIREMENTS

We define the expected goals that we want to achieve in our proposed security system in Mobile Ad-hocNetworks as follows:

4.1 Secure Ad-hoc Routing

Since the absence of a fixed infrastructure and central party, routing protocol in MANET be critical and vulnerable to some attacks, like described in Table 1. In order to prevent such attacks, it is important for the node to verify the authenticity of the other node and the integrity of the routing packets. In this work, we consider some security requirements to ensure the security of discovering routes and maintenance as follows :

Source Authentication : It ensures only authorized nodes are able to perform on the network. Nodes need to claimed and verified as authorized nodes. Without authentication mechanism, an adversary could masquerade a node, thus gaining unauthorized access toresources and sensitive information and interfering with the operation of other nodes.

Integrity : It ensures to keep the routing information from illegallynodes. Nodes need to be able to verify that the routing information is sent from legally nodes.

4.2 Secure Information Exchange

In MANET, the adversaries do not only attack adhoc routing. Data as payload also vulnerable from some some attacks such as modification, dropping and so on like described in Table 1. Here, we consider some security requirements berequired for constructing security system for information exchange in MANET as follows:

Data Integrity: No one user is able to access or modify, delete and reply the confidential data. It means the confidential data is guaranteed, safeguarding correctness of information.

Data Confidentiality: No one user is able to recover the original data, except the right users whose have a match attribute policy can decrypt the ciphertext. It means the exchange of the confidential data is kept undisclosed to others.

Authentication: It assurance that participants are authorized users. Communication participants must prove their identities to ensure the authenticity. If there is not an authentication mechanism, the adversary could act as the right user in that communication and thus get access to confidential data, or even spread some fake messages to disturb the network.

Access Control : It manages how people may access confidential data or other information using permission sets which allowing users access to information, namely access policy.

User Privacy/Anonymity : All privacy information is closely related to identity the owner should be kept private by the user itself and not be exposed to other.

5. PROPOSED SECURE INFORMATION EXCHANGE

In this section, we describe our proposed secure information exchange system in the scenario of military battlefield.

5.1 Our Approach

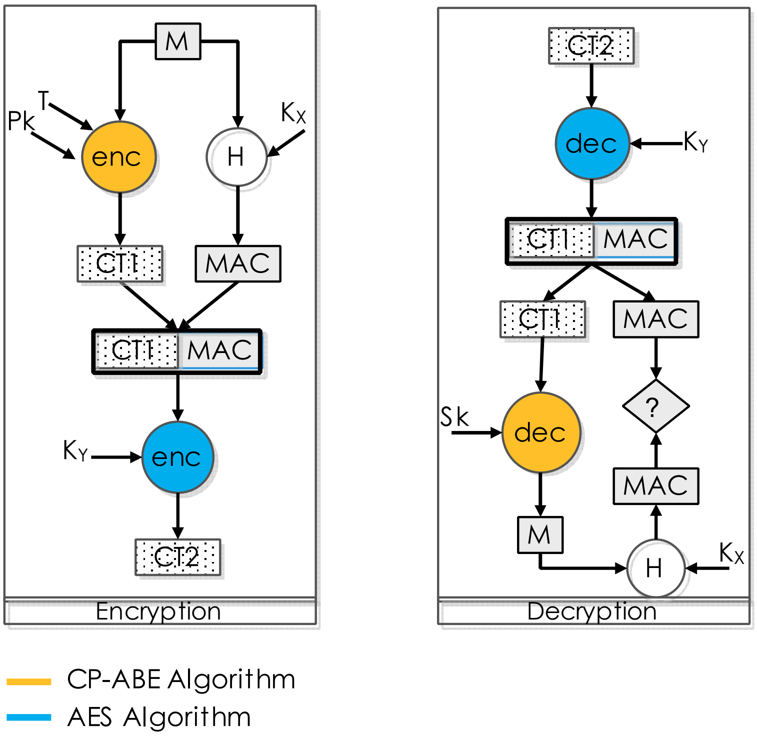

Figure 3. Our approach scheme

We have observed and reviewed our previous work [4] that in there occur a security hole that makes it vulnerable to attack. In that system, *MAC* as the output component from encryption phase which deliver to the receiver side in plaintext form like shown in Figure 2. If MITM can access the network and success to modify the *MAC*, the receiver will never get the correct data integrity. Consequently, receiver always feels that received data from invalid user. To solve that's problem, in this paper we propose to combine Authenticated-CPABE into AES to enhance the security level.The outputof Authenticated-CPABE will be encrypted by AES with shared key *K*. Then, message in ciphertext mode is transferred to the destination. In our implementation, we utilize AES with 256 bit key size to fulfill the security flaws and overcome the weaknesses of our previous approach.

As shown in Figure 3, the output information which would be delivered through a wireless link to the destination in ciphertext mode. As well as our previous work [4], we adopt setup and KeyGen algorithm from CP-ABE scheme [3]. The changed construction from Authenticated-CPABE algorithm in encryption and decryption phase. The first steps, running Authenticated-CPABE. Sender encrypts the message *M* using Authenticated-CPABE $Enc_{Auth\text{-}CPABE}(PK, T, M, K_X)$. It outputs *CT1* concatenate with *MAC*. The second steps, run AES encryption algorithm for encrypting the output from previous step with 256-bit shared symmetric key K_Y and resulting $CT2=Enc_{AES}(Enc_{Auth\text{-}CPABE}(PK,\ T,\ M,\ K_X),\ K_Y)$what deliver to receiver through radio link. It's computed as :

$$CT = Enc_{AES}\left[\begin{bmatrix} (\tau, \tilde{C} = M.e(g,g)^{\alpha Att}, C = h^{Att}, \\ \forall y \in Y:\ C_y = g^{q_y(0)}, C'_y = H\big(attr(y)\big)^{q_y(0)}\big), \\ MAC = H(M,K) \end{bmatrix}, k\right] \tag{6}$$

The receiver receives$CT2$ and decrypt it to get back the message M.Firstly, decrypt the $CT2$ uses AES and resulting $CT1CT1=Dec_{AES}(Dec_{Auth\text{-}CPABE}(PK,\ T,\ M,\ K_X),\ K_Y)$.Then, get back the message M using Authenticated-CPABE $Dec_{Auth\text{-}CPABE}(PK,\ T,\ M,\ K_X)$.It's computed as :

$$M = Dec_{AES}\left[\begin{bmatrix} \dfrac{C_{x}.A}{e(C2,D)} = \dfrac{C1.e(g,g)^{rAtt}}{e(h^{s}, g^{\alpha+r/\beta}} = \dfrac{M.e(g,g)^{\alpha Att}}{e(g,g)^{\alpha Att}}, \\ Verify(M,HMAC) = True/False \end{bmatrix}, k\right] \tag{7}$$

5.2 Security System

A MANET provides network connectivity between mobile nodes over potentially multihop wireless channels mainly through link-layer protocols that ensure one-hop connectivity, and network-layer protocols that extend the connectivity to multiple hops. These distributed protocolstypically assume that all nodes are cooperative inthe coordination process. This assumption is unfortunately not true in a hostile environment. Because cooperation is assumed but not enforced in MANETs, malicious attackers can easily disrupt network operations by violating protocol specifications.

We consider to implement our proposed scheme in a military environment. This military case study shows a battlefield in unknown territory, where infrastructure deployment is hard to achieve or maintain, therefore, MANET will be the perfect solution to such a scenario. As known, the military domain is a very challenging environment described by ambiguity and the need to be able to deal with significant anddisruptive dynamic changes. The military system goal is mainly concerned with the ability to satisfy a secure tactical information exchange for its environment, because the enemies are always trying their best to break down or destroy our activities. In a military consisting of different corps. Each one includes different elements, starting from a soldier to the commander-in-chief (officer).Military officer belonging to different categories (Captain, Lieutenants, Sergeants, Corporals, Soldier etc.) are divided into subgroups. Higher level officials can have access to the communication between its descendant lower level subgroups. Usually in the military, the officers will have a specific hierarchy, in which each officer will have the authority to give orders or to communicate with different elements based on his/her military ranking in the system.

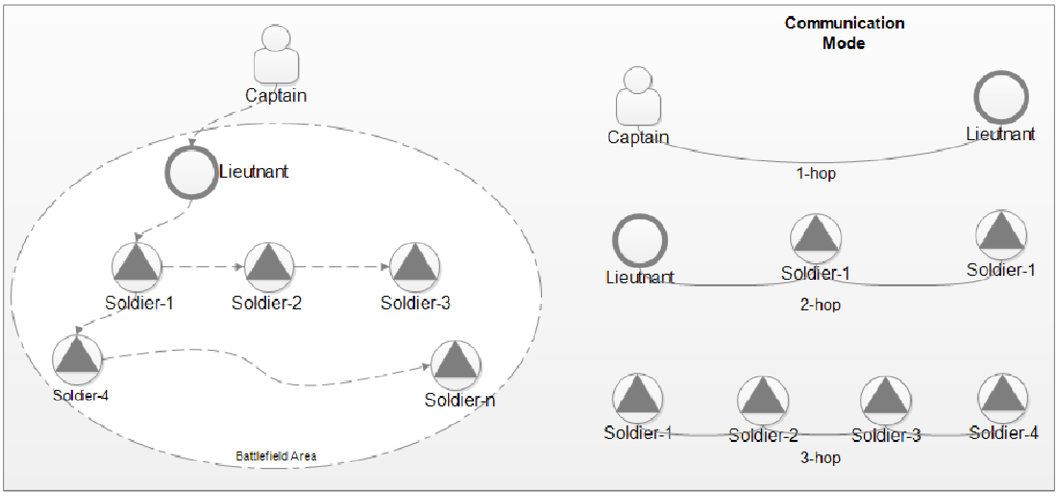

Figure 4. Proposed military case study scheme

The scenario used in this case study is in a simple war mission based on general operation [14] which involve higher level official, Captain as command center, lower level Lieutenant and soldiers. Captain as command center gives instructions orcommands fromoutside of battlefield to the lieutenantwho are in the same range. Then, lieutenant selecting commands from the captain, and forward that commands what addressed to the soldier by generated a new message with specific access policy. Our proposed scheme involves three parties: Captain, Lieutenant, and Soldiers like shown in Figure 4. All parties have the opportunity to act as an encryptor and decryptorfor exchanging information in a single hop and multi hop communication mode. Some confidential information may share in battlefield such as, strategy, tactics or commands from higher level official, ammunition status or health conditions from all parties in battlefield.

Captain. The entity who acts as Key Authority to generate all symmetric keys K and distributes to another participant in its below level. On other hand, Captain is a command center, all of commands related to war mission issued by captain.
Lieutenant. The entity who leads the soldiers in the battlefield area in a war mission. Lieutenant is one level below of captain. The lieutenant and captain are in within range, so theycan communicate directly without going through any intermediary.
Soldiers. The front-end parties.Itis the lower level office who face to face with the enemy. The soldiers communicate with the others in multi hop mode.

We define four protocols for implementation our proposed scheme : setup protocol, symmetric key distribution protocol, join and path establishment protocol and information sharing protocol.
Setup protocol. To act this protocol, we involve other entity out of participants, KGS. This protocol executed setup and key generation phases

which executed before MANET established. Setup and Keygen protocol areexecuted before MANET established with assume KGS and all participants within range of the network. This phase is illustrated in Figure5. We assume that there are secure and reliable communication channels within range of network between KGS and other parties during initial key setup and generation phases.We adopt the Setup and KeyGen algorithm of CP-ABE scheme [3]. Firstly, KGS operates setup algorithm which resulting *MK* and *PK*. Then, users who want to participate request their *SK* by attaching a set of user attributes *Att*. The attributes include corps, military rank level, position, and area. Based on the user attributes, KGS act KeyGen algorithm to generate each user secret key *SK*. Then distribute the public key *PK* and secret key of each user *SK-i*.

Next, We denote that Gateway (GW)representsas Captain, Node Coordinator (Co)representsas Lieutenant, and Node 1 until Node n represent as soldiers.

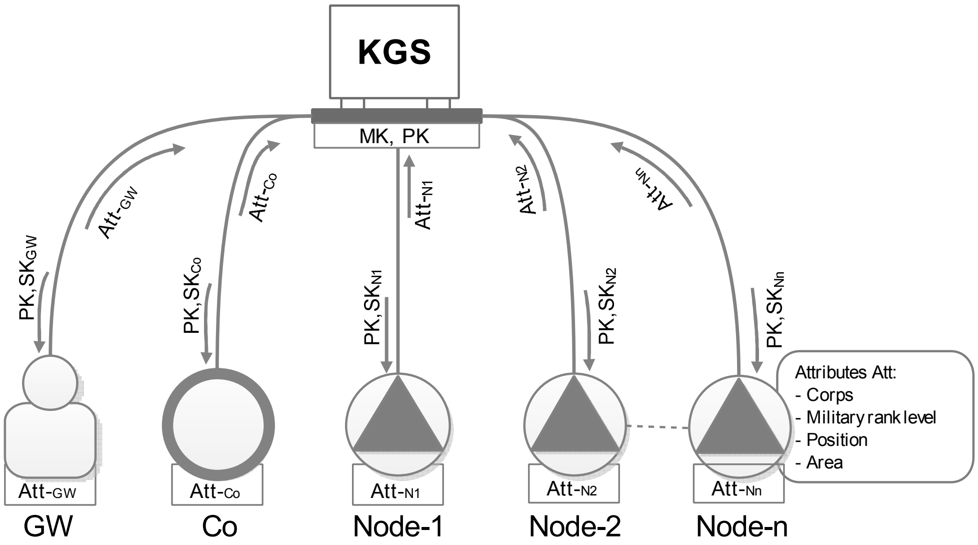

Figure 5. Illustration of the key generation phase.

Symmetric keys distribution protocol. In this section, the details of the proposed key distributionare presented. In the proposed key distribution, the goal is distributes symmetric keys to all authorized participating nodes as illustrated in Figure 6. This phase is executed on pre-processing with assume KGS and all participants within range of the network. In our system, we use different types of key to protect private content and control content access. There are four types of keys :

1. K_A : it is a 128-bit shared key PSK (Pre-Shared-Key) created by a user, used for user authentication joining the network in link layer based on WPA2-PSK-AES protocol.
2. K_B : it is a 128-bit shared key for HMAC-MD5 operation, used for routing packet authentication in network layer based on S-OLSR protocol.

3. K_C : it is a 256-bit shared key for HMAC-SHA256 operation to fulfill data integrity and authentication services.
4. K_D : it is a 256-bit shared symmetric key generated for AES encryption and decryption phases.

In this protocol,we adopt the encryption and decryption algorithms of CP-ABE scheme [3]. GW as Key Authority generates the symmetric keys$K$ (K_A, K_B, K_C, K_D). Then, distribute the symmetric keys$K$ securely using CP-ABE with the defined access policy. The symmetric keys$K$ (K_A, K_B, K_C, K_D) are encrypted using CP-ABE with the access policyT_1 to all participants (Co, Node 1, Node 2 until Node n). GW creates a ciphertext CT_K= $Enc_{\text{CP-ABE}}$ (PK, T_1, K), where $Enc_{\text{CP-ABE}}$ is the CP-ABE Encryption algorithm, and the access policy of attributes T_1. The Access policy *T1* structure as shown in Figure 7 can be represented as:

T_1 = ((‘SOLDIER’ AND ‘ARMY’) OR(‘LIEUTENANT’ OR ‘CAPTAIN’))

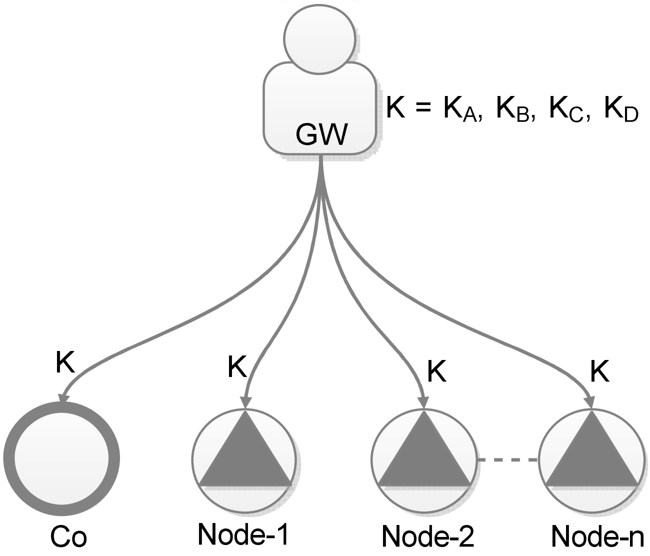

Figure 6. Illustration of symmetric keydistribution

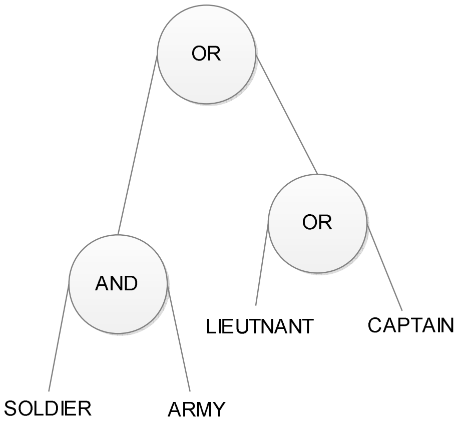

Figure 7. Access policy T_1 structure for symmetric keys distribution

After receiving CT_K, all authorized participantswhich satisfy the access policy T_1 can decrypt it to obtain the shared symmetric key Kusing CP-ABE Decryption algorithm.

Join and Path establishment protocol. By using the symmetric key K_A which obtained from the symmetric key distribution protocol, the joining participants will be ableto authenticate and claim as the legitimate participants to join a network which is applied WPA2-PSK-AES security system. After successfully joined in a network, participants are member of that network and connection established. The next step is path establishment phase. To establish a route towards the destination securely, we utilize S-OLSR protocol [11] which illustrated in Figure 8. Routing packets are distributed along with signature to ensure the integrity of routing packet and source authentication and time stamp to ensure the freshness of routing table and to prevent reply attack. Participants who have key K_B which from symmetric key distribution phase can authenticate and verify the packets hop-by-hop until the path is established.Only authorized participants can update the routing tables. Hence, in the established path, users can communicate and share any content with others privately.

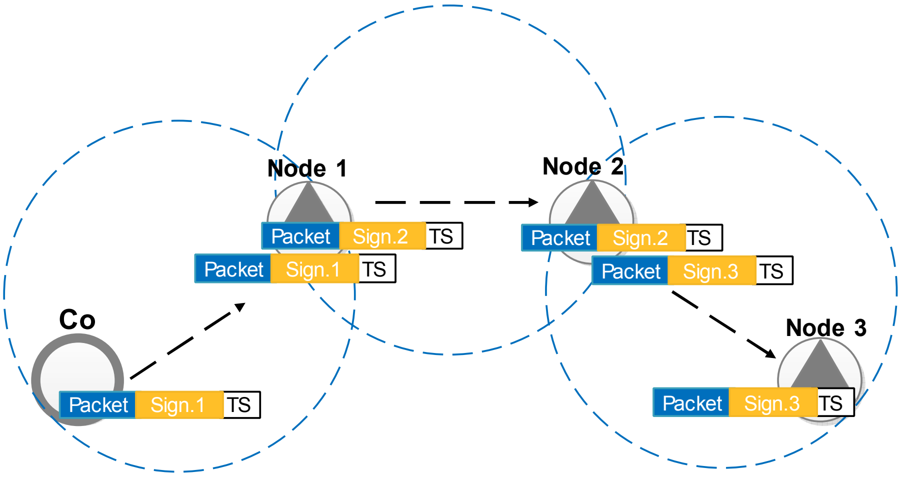

Figure 8. Illustration of path establishment phase based on S-OLSR

Information exchange protocol. This phase is only executed by all participants in the established path from source to destination. With the proposed security architecture like shown in Figure 3 we maintain and protect the data with fulfill some security services as described before. To cover our proposed security scheme and to highlight the implementation of secure information exchange mechanism in battlefield that described in above, we define different scenarios for exchanging information in a single hop and multi hop communication mode:

First Scenario. We consider that this scenario representedasingle hop communication. In this scenario, we assume that gateway GW and node coordinator Co within their range. Gateway as captaincan deliver some strategics command to node coordinatoras one below level official of gateway directly without multiple relaying mechanism.In here, GW as command center act as encryptor. GWencrypts the command*M* using the defined access policy $T_2CT_M = Enc_{AES}(Enc_{Auth\text{-}CPABE}(PK, T_2, M, K_C), K_D)$ and sends the ciphertext $CT_M$to a specific destination, Co. The data are transmitted via the established path. After receiving the encrypted data CT_M from GW, Co decrypts it to get back the original message*M*.The access policy T_2 like shown in Figure 10 is represented as:

T_2 = ((('ARMY' AND 'BATALYON.A') AND 'LIEUTENANT')OR'CAPTAIN')

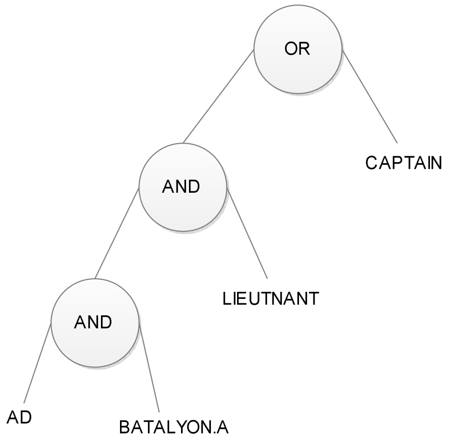

Figure 9. Access policy T_2 structure for information exchange in single hop mode.

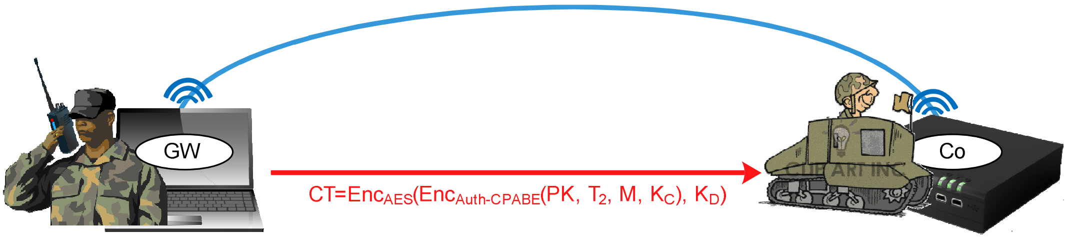

Figure 10. Experimental design of secure information exchange in single hop mode

Second Scenario. We consider that this scenario represented multi hop communication. In this scenario, sometimes a soldier run out of the ammo or shot, so make that the health condition dropped. Soldiers ask for help by sending confidentials message to other soldiers, and the leader in battlefiled, a lieutenant. In here, Node 3 act as encryptor. Node 3encrypts the message*M* using the defined access policy $T_3CT_M = Enc_{AES}(Enc_{Auth\text{-}CPABE}(PK, T_3, M, K_C), K_D)$ and sends the ciphertext $CT_M$to theothers who satisfy the access policy T_3. The encrypted message$CT_M$is transmitted via the established path. After receiving the encrypted messageCT_M, Node 1, Node 2 and Codecrypt it to get back the original message*M*.The access policy T_3 like shown in Figure 10 is represented as:

$$T_3 = ((\text{'SOLDIER' AND 'ARMY'}) \text{ OR 'LIEUTENANT'})$$

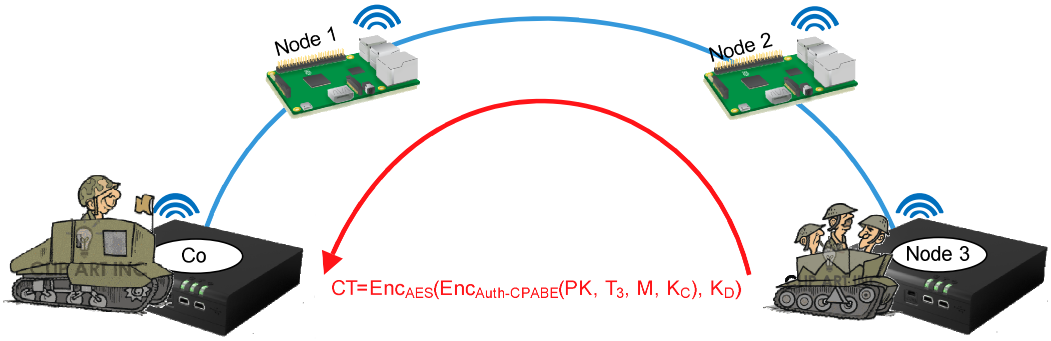
Node 1
Node 2
Co
Node 3
CT=Enc_{AES}(Enc_{Auth-CPABE}(PK, T₃, M, K_C), K_D)

Figure 11. Experimental design of secure information exchange in multi hop mode

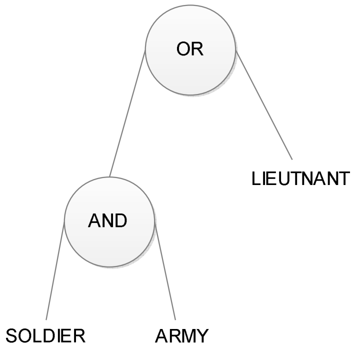

Figure 12. Access policy T_3 structure for information exchange in multi hop mode.

6. IMPLEMENTATION AND EXPERIMENTAL MEASUREMENTS

In this section, we describe our implementation of proposed secure information exchange in military environment and present the experimental results to confirm theeffectiveness of our proposed security scheme.

Act as participants in our implementation, We involve five mobile devices, act as gateway GW, node coordinator Co, and soldiers Node1, Node 2 and Node 3 . In our experiment, we use Laptop PC acts as GW and Fit-PC2i embedded computing and raspberry pi3 act as Co and Node1, Node 2, and Node 3. Moreover, the specification of Laptop PC, Fit-pc2i and raspberry pi3 are shown in Table 2.

Table 2. Hardware and Software Used in Experiment

Gateway GW	Node Coordinator Co & Node 3	Node1&Node 2
Laptop, Intel Core i3 2.4GHz, RAM 4GBDDR3, Wifi 802.11b/g/n, LinuxDebian kernel-3.5.0-17, gcc-4.7.2, gmp-5.1.1,pbc-lib-0.5.14, glib-2.34,openssl-1.0.1e, olsrd-0.9.0.3, s-olsr v.5.	Fit-pc2i, intel atom 1.6GHZ, RAM 2GB, Linux mint kernel-3.2.0-99, WLAN 802.11n,gcc-4.7.2, gmp-6.0.0, pbc-lib-0.5.14, glib-2.34,openssl-1.0.1e, olsrd-0.9.0.3, s-olsr v.5.	Raspberry pi3, armv7l 1.2GHz, RAM 1GB, Raspbian Wheezy 4.1.19,WLAN 802.11n, gcc-4.7.2, gmp-6.0.0, pbc-lib-0.5.14, glib-2.34,openssl-1.0.1e, olsrd-0.9.0.3, s-olsr v.5.

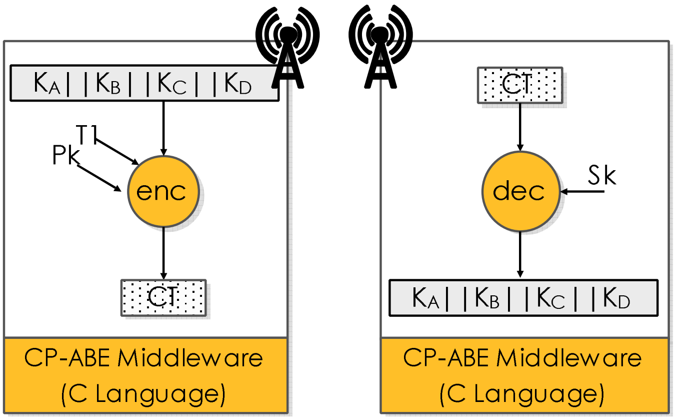

Figure 13. Implementation of secure symmetric key distribution

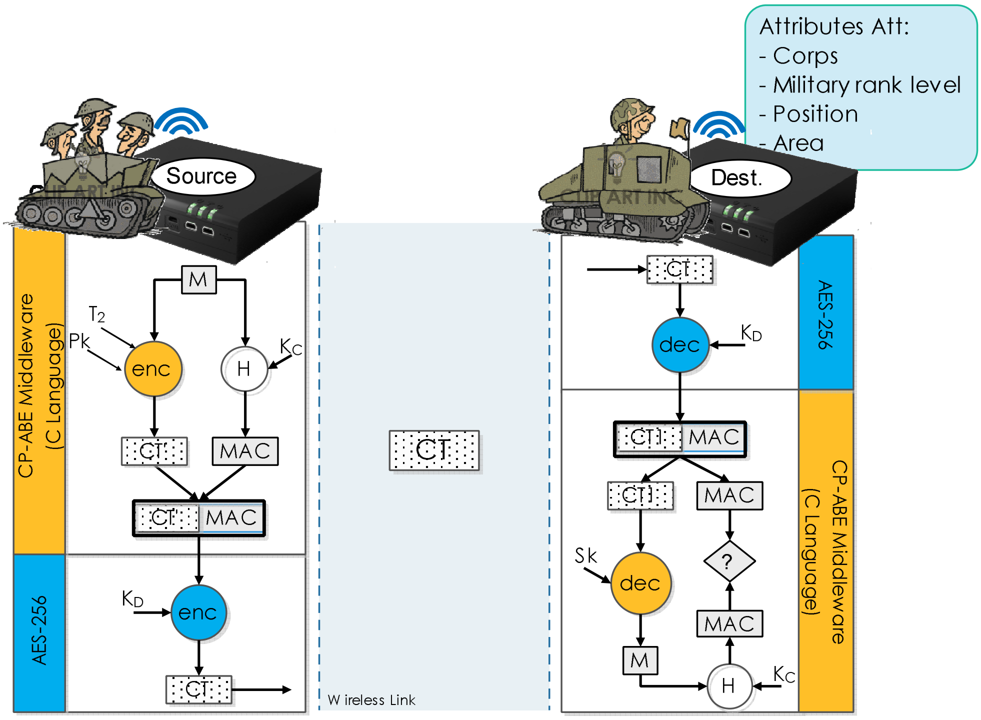

Figure 14. Implementation of secure information exchange system

Our implementation was built on native C programming. We adopted a middleware for the proposed scheme which is implemented on the PBC(Pairing-Based Cryptography) library. The PBC library[20] is for the pairing system and underlying ECC computations used in CP-ABE. The implementation of symmetric key distribution, and information exchange shown in Figure 13, and Figure 14. We implemented our proposed security scheme practically in around of PENS campus with the environment and the placement of nodes like shown in Figure 15.

In this work, we examined the proposed security scheme with measured the performance of our proposed security scheme in three main phases of the implemented system.

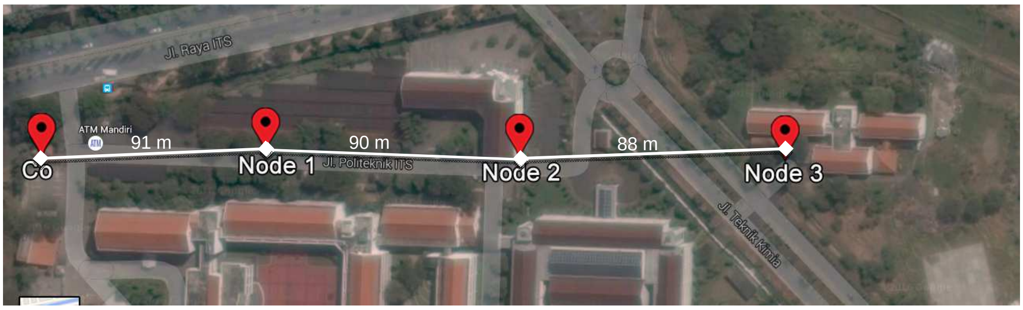

Figure 15. Test bed location and nodes placement

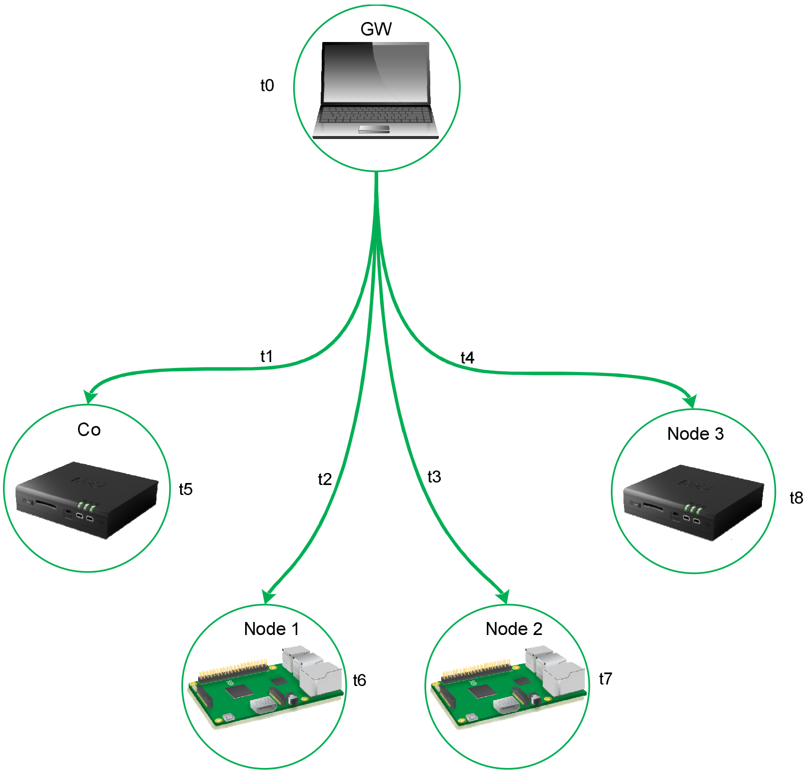

Figure 16. Time measurement of symmetric key *K* distribution

Measurement for Symmetric Key Distribution Phase

We measured the time consumption of symmetric key distribution phase. Gateway GW distributed the shared symmetric key K to all participants, Node Coordinator Co, Node 1, Node 2 and Node 3. The size of the shared symmetric key K and ciphertext are 96 Bytes and 1,555 Bytes, respectively. The scenario of time measurement for symmetric key K distribution is shown in Figure 16. The t0 is the time of CP-ABE encryption of symmetric key K on GW. The t1, t2, t3, and t4 are communication time to propagate encrypted key CT_K through IEEE802.11n Wireless connection. Meanwhile t5, t6, t7, and t8 are the time of CP-ABE decryption to extract and store the symmetric key K on Co, Node 1, Node 2, and Node 3, respectively. The total process of symmetric key distribution takes about 2,532ms, which is an accumulation of t0 to t8. The time of CP-ABE encryption for KwithT_1 is about 50.102 ms, the transmission time of CT_K is about 478ms, and CP-ABE decryption time for recovering Kt5,t6,t7, and t8 are about 100 ms,179.839 ms, 179.839 ms and 100 ms respectively.

Measurement for Path Establishment Phase

We measured the processing times for updating the routing table based on S-OLSR protocol until the path established with the topology scenario shown in Figure 17. We assume that Co is the routing-initiator node. The total time of routing message exchange on 3-hop until the path established is about 997ms.

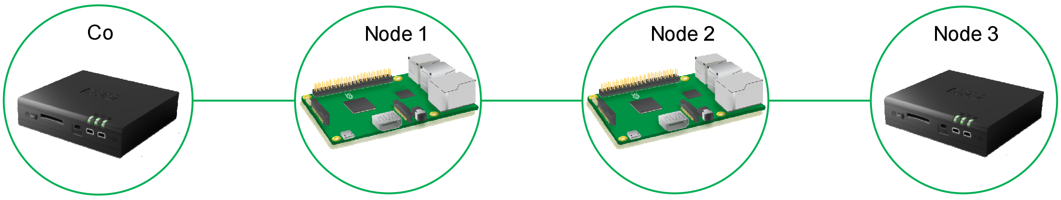

Figure 17.Path establishment topology

Measurement for Information Exchange Phase

We measured the time consumption of information exchange phase with different message sizes and types in different scenarios. The size of shared informations in batlefield area relatively not so big. There is possible that the informations in image type, for example photo of battlefield condition.We measured the time consumption with 50Bytes, and 1000Bytes text data type and image data type. Table 3 shows the total times of transferring various types of data with first scenario in single hop mode using proposed scheme based on access policy T_2. The encrypted Information Exchangeprocess illustrated in Figure 10.

After establishing the path, we transfer various data using two scenarios which represented single hop and multi hop communication mode. With the first scenario, where GW and Co are within their ranges, To exchange a text file with size 50 Bytes, it totally takes about 690ms, which consists of about 40.076 ms for the CP-ABE encryption at GW, about 470ms for the transmission, and about 180.374 ms for the CP-ABE decryption at the Co. The encryption time and decryption time are relatively stable, even for exchanging the text file with data size1,000 Bytes. These take 50.742 ms and 190.649 ms, respectively. However, the transmission time becomes 713ms. To exchange the image file with 2,256,451Bytes takes about 4,874 ms, where the encryption time and decryption time are about 120.613 ms and 520.263 ms, respectively. Meanwhile, the transmission time takes 4,233ms.The increases of ciphertext size for this scenario is around 1,520 Bytes like shown in Figure 18.

Table 3. Processing times for exchanging various datain the first scenario

Original data size, encrypted data size	Encryption, transmission, decryption, times (ms)	Total processing time (ms)
Text file		
50 Bytes, 1,573 Bytes	40.076 470 180.374	690.450
1,000 Bytes, 2,517 Bytes	50.742 713 190.649	954.388
Image file		
2,256,451 Bytes, 2,257,973 Bytes	120.613 4,233 520.263	4,873.876

Table 4. Processing times for exchanging various data in the second scenario

Original data size, encrypted data size	Encryption, transmission, decryption, times (ms)	Total processing time (ms)
Text file		
50 Bytes, 1,280 Bytes	290.133 1,290 160.421	1,740.554
1,000 Bytes, 2,224 Bytes	300.830 2,976 170.746	3,447.576
Image file		
2,256,451 Bytes, 2,257,680 Bytes	520.563 12,118 480.131	13,118.694

For the second scenario, we measured the time consumption of information exchange in multi hop communication mode with experimental design like shown in Figure 11. Node 3 wants to share information to Co (3-

hop). To exchange a text file with size 50 Bytes, it totally takes about 1,741ms, which consists of about 290.133 ms for the CP-ABE encryption at Node 3, about 1,290ms for the transmission, and about 160.421 ms for the CP-ABE decryption at the Co. The encryption time and decryption time are relatively stable, even for exchanging the text file with data size 1,000 Bytes. These take 300.830 ms and 170.746 ms, respectively. However, the transmission time becomes 2,976ms. To exchange the image file with 2,256,451Bytes takes about 13,119ms, where the encryption time and decryption time are about 520.563 ms and 480.131 ms, respectively. Meanwhile, the transmission time takes 12,118 ms. The increases of ciphertext size for this scenario is around 1,227 Bytes like shown in Figure 18.

Table 5. Processing times for exchanging various data in other possibilities

	Original data size, encrypted data size	Encryption, transmission, decryption, times (ms)	Total processing time (ms)	Encryption, transmission, decryption, times (ms)	Total processing time (ms)
		Co-Node 1 (1-hop)		Co-Node 2 (2-hop)	
Text	50 Bytes, 1,280 Bytes	290.133 457 159.646	906.779	290.133 890 159.646	1,339.779
	1,000 Bytes, 2,224 Bytes	300.830 715 168.490	1,184.320	300.830 1,376 168.490	1,845.320
Image	2,256,451 Bytes, 2,257,680 Bytes	520.563 4,233 359.636	5,113.199	520.563 8,118 359.636	8,998.199
		Node 1-Node 2 (1-hop)		Node 1-Node 3 (2-hop)	
Text	50 Bytes, 1,280Bytes	190.073 452 159.646	801.719	190.073 895 160.421	1,245.494
	1,000 Bytes, 2,224Bytes	292.433 705 168.490	1,165.923	292.433 1,382 170.746	1,845.179
Image	2,256,451 Bytes, 2,257,680 Bytes	338.726 4,233 359.636	4,931.362	338.726 8,120 480.131	8,938.857
		Node 2-Node 3 (1-hop)		Co-Node 3 (3-hop)	
Text	50 Bytes, 1,280Bytes	190.073 461 160.421	811.495	290.133 1,290 160.421	1,740.554
	1,000 Bytes, 2,224Bytes	292.433 719 170.746	1,182.179	300.830 2,976 170.746	3,447.576
Image	2,256,451 Bytes, 2,257,680 Bytes	338.726 4,240 480.131	5,058.857	520.563 12,118 480.131	13,118.694

As the defined access policy T_3, users who can decrypt the ciphertext CT_M are soldiers and lieutenant. So, there are several possibilities for data exchange scheme, both among soldiers and soldier with lieutenant. Table 5 displays the times for exchanging various data in other possibilities. As shown in Table 3, 4 and 5, the transmission time increases as the exchanged data is larger. Table 6 and 7 show the performance of encryption time and decryption time of 50 Bytes data. The additional of HMAC and AES schemes using processor 1.2GHz only take processing time about 4.452 ms, we can confirm that our approach by using CP-ABE with added HMAC and AES schemes make low overhead.

Table 6. Performance of the encryption time of 50 Bytes data

Type of Devices	Processing time (ms)			Total (ms)
	CP-ABE	HMAC-256	AES-256	
Laptop	39.317	0.036	0,724	40.076
Fit-PC2i	288.229	0.538	1.366	290.133
Raspberry pi3	188.184	0.533	1.356	190.073

Table 7. Performance of the decryption time of 50 Bytes data

Type of Devices	Processing time (ms)			Total (ms)
	CP-ABE	HMAC-256	AES-256	
Laptop	19.269	0.035	0.988	20.292
Fit-PC2i	157.749	0.536	2.136	160.421
Raspberry pi3	157.085	0.533	2.028	159.646

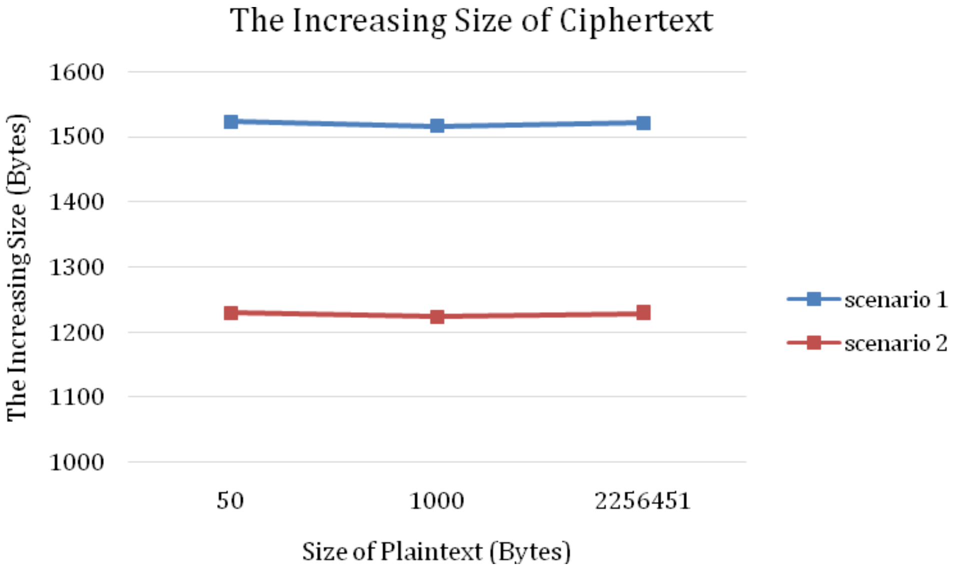

Figure 18. The increasing size of ciphertext

Table 8 shows the comparison between the design of the proposed scheme and related works based on some parameters : security requirements, key distribution protocol, realization, mode and secure layer.

Table 8. Comparison between the design of the proposed scheme and related works

		[15]	[19]	Proposed Scheme
Security requirements	Data Integrity	yes	no	yes
	Data Confidentiality	yes	yes	yes
	Authentication	yes	yes	yes
	Access Control	no	yes	yes
	User Privacy	no	yes	yes
Key Distribution Protocol		yes	yes	yes
Realization		Design	Real test bed	Real test Bed
Mode		Multi hop	Multi hop	Single hop and multi hop
Secure layer		Application layer	Network layer	Network and application layers

Assume there is a MITM (Meet In The Middle) between the communicating nodes which potentially for intercepting and compromising the messages sent. In the set up of the communication between nodes, it is required to have shared key K_A and K_B for joining the secured network WPA2-PSK-AES and S-OLSR based. So, the network is only decrypted and authenticated by nodes who have K_A and K_B for joining the network. A MITM may not only passively intercept the communication, but also actively attacks such as access, modificate, or remove the content of the communication. Even if this phase can be penetrated and then he has K_D to decrypt the ciphertext *CT2*, he would feel cheated or deceived because he cannot read the confidential message, only get the ciphertext form *CT1* from the real confidential message. So, If the message from the nodes is encrypted with *PK* and K_C, then the message is only decrypted with the corresponding key, *SK* and Kc. Because the*SK* only owned by the legitimated node which makes it impossible for attacker to decrypt a message without have any additional information like the registered user attributes and the access policy used. Although this system can be used to prevent the threat of attacks and fairly safe, but it is still evaluated on the current scenarios of implementations and the current conditionof devices. Moreover, an absolutely secure system cannot be reached and the threat for security system always keep abreast.

7. CONCLUSION

We have presented a secure communication information exchange in Mobile Adhoc Network (MANET) system and its implementation which offers secure in adhoc routing and information exchange. We also design protocols to implement the proposed scheme for various battlefield scenarios in real environment using embedded devices.The combination of Authenticated-CPABE with the symmetric cryptography algorithm increase the robustness of the proposed secure model.The experimental results show the practicality of the proposed system in the current environment of embedded devices. The transmission time dominated of total processing time on the proposed security system. Experimental results show that the additional of HMAC and AES schemes using processor 1.2GHz only take processing time about 4.452 ms, we can confirm that our approach by using CP-ABE with added HMAC and AES schemes make low overhead. This system can be used to prevent the threat of attacks and fairly safe, but it is still evaluated on the current scenarios of implementations and the current conditionof devices.

Our plans for future work include but are not limited to provide key management protocol, such as key renewal and revocation mechanisms.

Acknowledgements

The project has received research funding from LPDP (Indonesia Endowment Fund for Education) through thesis and dissertation scholarship schemeNo. PRJ-660 /LPDP.3/2016.

REFERENCES

[1] H.Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, **Security in Mobile Ad hoc Networks: Challenges and Solutions**, *IEEE Wireless Communications*, pp. 38-47, 2004.

[2] W. Stalling, **Network Security Essentials: Applications and Standards**, *Prentice Hall Press*, 4th edition, ISBN-13: 978-0136108054, 2010.

[3] J. Bethencourt, A. Sahai, and B. Waters, **Ciphertext-Policy Attribute-Based Encryption**, *IEEE Symposium on Security andPrivacy*,pp. 321-334, 2007.

[4] S. Huda, A. Sudarsono, and T. Harsono, **Secure Data Exchange using Authenticated Ciphertext-Policy Attributed-BasedEncryption**, *17th International Electronics Symposium*,Surabaya, pp. 140-145, 2015.

[5] A. Sudarsono, and T. Nakanishi, **An Implementation of Secure Data Exchange in Wireless Delay Tolerant Network using Attribute-**

Based Encryption, *2nd International Symposium on Computing and Networking*,Shizuoka, pp. 536-542, 2014.

[6] J.H. Chen, Y.T.Wang, and K. Chen, **Attribute-Based Key-Insulated Encryption**,*Journal of Information Science and Engineering*, Vol.27, pp. 437–449, 2011.

[7] A. Sudarsono, and T. Nakanishi, **An Implementation of Secure Data Exchange System with Multi-hop Routing in Wireless Delay Tolerant Network Using Attribute-Based Encryption**, *3rd International Symposium on Computing and Networking*, Hokkaido, pp. 470-476, 2015.

[8] X. Guo, T. Feng, J. Fang, J. Wang, and Y. Lu, **Secure Content Delivery Scheme Based on Yaksha System for CCMANETs**,*Journal of Communications*, Vol.11, No. 2, pp. 221-230, 2016.

[9] K. Zeng, S. Yu, K. Ren, W. Lou, and Y. Zhang, **Towards Secure Link Quality Measurement in Multihop Wireless Networks**, *2008 IEEE Global Telecommunications Conference*, pp. 1 – 5, 2008.

[10] C. Panos, P. Kotzias, C. Xenakis, I. Stavrakakis, **Securing the 802.11 MAC in MANETs: A Specification-Based Intrusion Detection Engine**, *9th Annual Conference on Wireless On-Demand Network Systems and Services*, Courmayeur, pp. 16 - 22, 2012.

[11] A.Hafslund, A.Tonnesen, R.B.Rotvik, J.Andersson,and O.Kure, **Secure Extension to the OLSR Protocol**,*OLSR Interop and Workshop*, pp. 1-4, 2004.

[12] A. Sudarsono, **Anonymous On-Demand Routing Protocol using Pairing-Based Group Signature**,*Industrial Electronic Seminar*,Surabaya, pp. 76-84, 2013.

[13] Z. Wan K. Ren, B. Zhu, B. Preneel, and M. Gu, **Anonymous User Communication for Privacy Protection in Wireless Metropolitan Mesh Networks**,*IEEE Transactions on Vehicular Technology*, Vol.59, No. 2, pp. 519-532, 2010.

[14] R.Roy and M.Chuah, **Secure Data Retrieval Based on Ciphertext PolicyAttribute-Based Encryption (CP-ABE) System for DTNs**, Journal of Cryptology, vol. 17, No.4, pp.297-319,2004.

[15] A.A Yavuz, F. Alagoz, and E. Anarim,**A New Multi-tier Adaptive Military MANET Security Protocol using Hybrid Cryptography and Signcryption**, Turkish Journal of Electrical Engineering & Computer Sciences, Vol.18, No.1, pp.1-22, 2010.

[16] E.A. Panaousis, T.A. Ramrekha,and C. Politis, **Secure Routing for Supporting Ad-hoc Extreme Emergency Infrastructures**,*The Future Networkand Mobile Summit 2010 Conference*,Place, pp. 1-5, 2010.

[17] M. Winkler, K. Tuchs, K. Hughes, and G. Barclay, **Theoretical and Practical Aspects of Military Wireless Sensor Networks**,*Journal of Telecommunications and Information Technology*, Vol. 2, pp. 37-45, 2008.

[18] H. Kwon, C. Hahn, D. Kim, K. Kang, and J. Hur, **Secure Device-to-Device Authentication in Mobile Multi-hop Networks**,*9th International Conference on Wireless Algorithms, Systems, and Applications*, pp. 267–278, 2014.

[19] H. Kwon, D. Kim, C. Hahn, and J. Hur, **Secure Authentication using Ciphertext Policy Attribute-Based Encryption in Mobile Multi-hop Networks**,*Multimedia Tools and Applications*, pp.1-15, 2016.

[20] J. Bethencourt, A. Sahai, and B. Waters, **CPABE Toolkit in Advanced Crypto Software Collection**,http://hms.isi.jhu.edu/acsc/cpabe/ [accessed on February, 2016].

[21] B.Lynn, **PBC (Pairing-Based Cryptography) Library**,http://crypto.stanford.edu/pbc, [accessed on February, 2016].

[22] **Libgcrypt-Standalone HMAC-256 Implementation**,http://svn.cubrid.org/cubridengine/trunk/external/libgcrypt-1.5.2,[accessed on February, 2016].