Turkish Journal of Electrical Engineering and Computer Sciences

Volume 18 | Number 1 Article 1

1-1-2010

A new multi-tier adaptive military MANET security protocol using hybrid cryptography and signcryption

ATTİLA A. YAVUZ

FATİH ALAGÖZ

EMİN ANARIM

Turk J Elec Eng & Comp Sci, Vol.18, No.1, 2010, © TÜBİTAK
doi:10.3906/elk-0904-6

A new multi-tier adaptive military MANET security protocol using hybrid cryptography and signcryption*

Attila A. YAVUZ[1], **Fatih ALAGÖZ**[2], **Emin ANARIM**[3]
[1]*Department of Computer Science, NC State University*
North Carolina, Raleigh, NC 27695, U.S.A.
e-mail: aayavuz@ncsu.edu
[2]*Department of Computer Engineering, Bogazici University*
Bebek, İstanbul 34342, TURKEY
e-mail: alagoz@boun.edu.tr
[3]*Department of Electrical and Electronic Engineering, Bogazici University*
Bebek, İstanbul 80815, TURKEY
e-mail: anarim@boun.edu.tr

Abstract

Mobile Ad-hoc NETworks (MANETs) are expected to play an important role in tactical military networks by providing infrastructureless communication. However, maintaining secure and instant information sharing is a difficult task especially for highly dynamic military MANETs. To address this requirement, we propose a new multi-tier adaptive military MANET security protocol using hybrid cryptography and signcryption. In our protocol, we bring novelties to secure military MANET communication for three main points: Cryptographic methods used in MANETs, hybrid key management protocols and structural organization of the military MANETs. As a new approach, we use hybrid cryptography mechanisms and Elliptic Curve Pintsov-Vanstone Signature Scheme (ECPVSS) that provide security and performance advantages when compared to some traditional cryptographic methods. Furthermore, multi-leveled security approach of our protocol provides adaptive solutions according to the requirements of different military units in the MANET. We also use a hybrid key management technique that combines the benefits of both decentralized protocols with single point of failure resistivity and centralized protocols with low rekeying cost. Last, the proposed network structure facilitates certification and key management for the MANET by providing flexibility for Mobile Backbone Network (MBN) tiers.

Key Words: *Network Security, Military Ad-hoc network, Cryptography, Signcryption, Multi-tiered Structures.*

*A preliminary version of this paper was published at ISCIS'06 [1].

1. Introduction

Network centric warfare broadly describes the combination of strategies, emerging tactics, techniques, procedures and organizations, which allow even a partially networked force to gain a decisive warfighting advantage. Network centric warfare should be supported with capabilities such as mobility, security, survivability, and is capable of supporting multimedia tactical information [5]. This requires the importance of secure, integrated and efficient networking in Digital Battle Fields (DBFs), which may be comprised of various critical networking components including satellites, terrestrial units and tactical operation centers. Among them, military Mobile Ad-hoc NETworks (MANETs) gain a special importance for the future combat systems. MANETs are infrastructureless wireless communication networks and they are considered as an ideal technology for the instant communication in both military and civilian applications. Tactical military networks, requiring high security and performance together, are one of the main application areas of MANETs. Operating in hostile environments and the infrastructureless characteristics of MANETs make these networks vulnerable to various types of attacks.

In this study, in order to address these problems, we propose a new multi-tier adaptive military MANET security protocol using hybrid cryptography and signcryption. In our protocol, we particularly focus on the secure multicast concept to provide secure and instant communication in a Digital Battle Field (DBF). In order to provide security and efficiency simultaneously, we make contributions to the military MANETs for three main areas: Structural design of the military MANET, cryptographic methods used in MANETs and integrated key management techniques. These areas are particularly selected, since they are essential factors that determine security and performance characteristics of the military MANETs. We use a multi-tiered network structure, which provides advantages for structural organization of military MANETs. Two tiered Unmanned Aerial Vehicle-Mobile Backbone Networks (UAV-MBN) have been recently proposed for DBFs exploiting the heterogeneous structure of military MANETs [6], [7]. In our protocol, as a new approach, we divide MBN tier into MBN1 and MNB2 tiers. This significantly facilitates key management, since it encapsulates effects of the rekeying operation in the restricted sub-theaters. It also utilizes some benefits of MBN1 type nodes and facilitates certification procedures in the MBN tier by reducing the threshold cryptography requirements. Particularly, when UAVs are not available in the military MANET for any reason, this structure provides flexibilities when compared to the traditional approaches.

Various cryptographic methods have been proposed in order to secure MANETs [8]. In a secure MANET, availability, confidentiality, integrity, authentication, unforgeability and non-repudiation goals must be achieved [9]. In our protocol, as a novel approach, we use signcryption type key exchange scheme Direct Key Exchange Using Time Stamp (DKEUTS) [10] and Elliptic Curve Pintsov-Vanstone Signature Scheme (ECPVSS) [11] as the building block methods. An efficient integration and adaptation of these methods to the aforementioned structure brings all basic cryptographic services together. This approach also reduces communication (bandwidth usage) and computational overheads, when compared to classical methods. DKEUTS is suitable for fair key exchange among high level tiers of military MANETs, while ECVPSS is used for bandwidth/computational resource limited Regular Ground Nodes (RGN). The proposed multi-leveled security mechanism provides sufficient security for each tier, while prevents the network from being overloaded due to the unnecessary cryptographic operations.

In key management aspect, we propose a hybrid key management technique, which can scale very large and dynamic military MANETs. We adapt principles of independent tiers for TTPVSS [12], three tiered satellite

multicast security protocol [13] and NAMEPS [14] to military MANETs. These approaches significantly reduce workload of the rekeying, which is required to provide forward and backward security. Also, single point of failure problem is minimized by using hybrid key management structure. Note that key management principles of these protocols can not be applied directly to Ad-hoc networks due to the lack of permanent infrastructure. Thus, we adapt them by taking into consideration structural design properties of the military MANETs.

The rest of the paper is organized as follows. Section 2 gives related works and background for cryptographic methods and key management techniques used in our protocol. Section 3 presents structural design of our protocol. Section 4 presents cryptographic techniques and multi-level security approach. Section 5 provides detailed steps of our protocol by describing mathematical transformations associated with the each tier. Section 6 gives analysis of our protocol for three main aspects such as advantages of the preferred cryptographic and hybrid key management techniques and properties of the new network structure. Conclusion and future works are given in Section 7.

2. Related works and background

In this section, we present related works and background information for cryptographic techniques and key management protocols used in Ad-hoc networks.

2.1. Cryptographic techniques used in Ad-hoc networks

In order to provide main cryptographic goals in Ad-hoc networks, various cryptographic methods based on the public key and hybrid cryptography have been proposed. In Ad-hoc network, due to the lack of infrastructure, a static Trusted Third Party (TTP) may not be available continuously. Thus, key exchange and key establishment schemes based on Diffie-Hellman (DH) [15] variants are frequently used for collaborative key exchange. Especially, for hierarchical key agreement in Ad-hoc networks, extending DH to the groups, Group Diffie-Hellmann (GDH)-1-2 [16] protocols are used. Hypercube, Octopus and Burmester-Desmedt protocols are also used for a hierarchical group key exchange [17]. Furthermore, key agreement protocols using generic password-based authenticated key exchange schemes and DH variants with extensions to the multi-party versions have been suggested in [8]. There are other protocols using variants of these approaches (e.g., [18]).

Another important technique, which is frequently used in Ad-hoc network security, is the threshold cryptography [19], [20]. Threshold cryptography is to construct a distributed public key management service to solve trusted certification problems. Hence, if some components of the system are compromised, Single Point of Failure (SPoF) problem will not occur for certification issues. In [9], a distributed public-key management service for Ad-hoc networks has been proposed using aforementioned techniques.

2.2. Group key management protocols

Key management is one of the most important issues in security protocol design. In a secure group communication, key management techniques are used to provide correct distribution and easy maintenance of cryptographic keys. Note that secure multicast applications are the most common form of the group communication and they are especially important for military MANETs.

In multicast communication, a central entity transmits the same message to a group of members.

Since bulk data multicast applications are the most common form of the multicast, symmetric cryptography based techniques are frequently used to encrypt the bulk data. However, these techniques require the secure distribution of the symmetric keys between group members. As discussed in Section 2.1, hybrid cryptography is used together with key management protocol to achieve desired cryptographic goals. Group Key (GK) is used to encrypt bulk multicast data. Every member in group knows GK and can decrypt multicast data using GK. However, GK must be transmitted to members securely. A key exchange scheme or other public key cryptography based methods are used for this purpose. The cryptographic keys, which are used to encrypt GK, are called as Key Encryption Key (KEK). Thus, key management problem can be considered as the secure and efficient distribution of KEKs and GK to only valid members. However, majority of the multicast systems have large and dynamic groups, in which member join-leave events are frequent. Hence, a key management protocol must be able to handle cryptographic workload resulting from large and dynamic structure of the group and should provide freshness of the cryptographic key in the network [21]. In large multicast systems, most costly operation is the rekeying, whose purpose is to forward and backward security in the network [22], [23].

Various key management protocols have been proposed to solve problems of key management in large and dynamic groups. We can classify group key management protocols into three main categories: Centralized, decentralized and hybrid key management protocols [24], [25].

In centralized group key management protocols, there is only one central entity (TTP) that controls the whole group. No auxiliary entity is required to perform key distribution. Key-tree based centralized protocols, which scale group size logarithmically, are the most frequently used techniques in the centralized protocols. Logical Key Hierarchy (LKH) [26], One-Way Function Tree (OFT) [27], and Efficient Large Group Key (ELK) [28] are well-known protocols using these approaches. In order to achieve computational advantages for rekeying operation, each of these protocols uses logical key tree based approaches. However, centralized methods described above are vulnerable to SPoF problems.

In contrast to centralized techniques, decentralized group key management protocols split the large group into small sub-groups. Different controllers are used for each sub-group. Using modularity principle, large group can be handled with different key management protocols operating independently in each of sub-groups. Since the system does not depend on a single group manager, decentralized key management protocols are not vulnerable to SPoF problem. Iolus [29] is a representative example of such a protocol.

Hybrid protocols integrating these two approaches can be found in [12], [13] and [14]. Note that even if [12], [13] and [14] focus on satellite multicast systems, hybrid key management techniques of these studies can be applied to any large and dynamic network system. In [12], two tiered structure, Two-tier Pintsov-Vanstone Signature Scheme (TTPVSS), has been proposed using LKH in each of its tiers. TTPVSS uses independence of tiers principle and effect of modifications, which are performed over single point of the network, are restricted in local regions. Other parts of the network and especially the central manager are not affected from modifications. This provides significant performance gain for the central manager (satellite in that case). The study in [13] extends principles of TTPVSS to three-tiered structure and utilizes some properties of existing hierarchy in satellite networks. Validation ticket mechanism has been introduced to lower tiers in order to facilitate key management and roaming among Terrestrial Units (TU) for regular members. Notice that we inherit this mechanism to our MBN2-RGN tier and elite RGN units so that they can gain direct access to UAVs in critical situations. Another hybrid key management solution for multi-tiered secure multicast applications can be found in N-tiered Satellite Multicast Security Protocol based on signcryption Schemes (NAMEPS) [14]. Different from

[12] and [13], NAMEPS uses ELK key management protocol, which provides advantages for member leave events. We also use ELK key management protocol in our protocol for each individual theater. The benefits of ELK integration in our protocol are given in Section 6.2.

3. Structural design of the proposed protocol

In this section, we first give the structural design of the classical UAV-MBN military MANETs and then present details of the structural design of our protocol.

3.1. UAV-MBN military MANETs

General purpose ad-hoc network protocols are based on the homogeneous network assumption (especially for routing aspect) [30]. In this assumption, all nodes are accepted as if they have similar transmission, computational and storage capabilities. However, as denoted in [31], the homogeneity assumption creates performance problems such as traffic overhead resulting from on-demand routing approach [32]. In addition, theoretical studies related to throughput bounds of the homogeneous ad-hoc wireless networks state that under uniform traffic pattern, the available bandwidth to each node approaches zero as the network size increases [7], [33]. Note that military ad-hoc networks already have a highly heterogeneous network structure with partially or completely infrastructureless properties. Existing hierarchical structure of military networks also contributes to the heterogeneity assumption. According to their task in the battlefield, each component of the military network has their special communication, computational and storage capabilities. Thus, the homogeneity assumption is not valid for the military ad-hoc networks.

Addressing these problems, UAV-MBN networks have been proposed exploiting the heterogeneous structure of military ad-hoc networks [6], [34]. UAV-MBN networks have three-tired structure based on computational and communication capabilities of the networking units (see Figure 1). UAV-MBN networks consist of three main tiers as UAVs, MBN and RGN tiers. The UAV tier consists of an aerial mobile backbone having UAVs in a circle with a diameter of around 8 nautical miles. UAVs [35] have a critical importance in the modern battlefield communications. Small low-Cost commercial off-the-shelf (COST) radio equipment combined with powerful computer processing can be integrated on an UAV in order to form a multi-UAV, tactical-UAV and swarming UAV based MANETs for both military and commercial applications. UAVs have high communication capabilities such as phased arrayed antennas so that they can communicate with lower tier units in military MANETs. In this structure, each UAV is responsible for its own specific battlefield sub-region (theater). Second tier of the UAV-MBN network includes MBN type nodes, which are classical land force units such as tanks and armored personnel carriers. These vehicles have strong communication and computational capabilities together with beam-forming antennas. MBN tier provides a backbone for purely infrastructureless components of the network and integrate UAV tier to the purely infrastructure-less RGN tier. Third tier of the UAV-MBN network is the RGN tier. RGN tier comprises of soldiers equipped with limited communication and computation devices. RGN tier is generally purely infrastructureless [7]. In fact, if appropriate key management techniques and cryptographic methods are not used, UAV-MBN type military MANETs may face with serious security and performance problems. MBN tier requires a distributed trust mechanism that may cause performance deterioration. Also, especially for UAV and MBN tiers, SPoF problem may arise. Detailed analysis of aforementioned

problems and advantages of our solutions are provided in Section 6. In the next part, we describe structural design properties of our protocol.

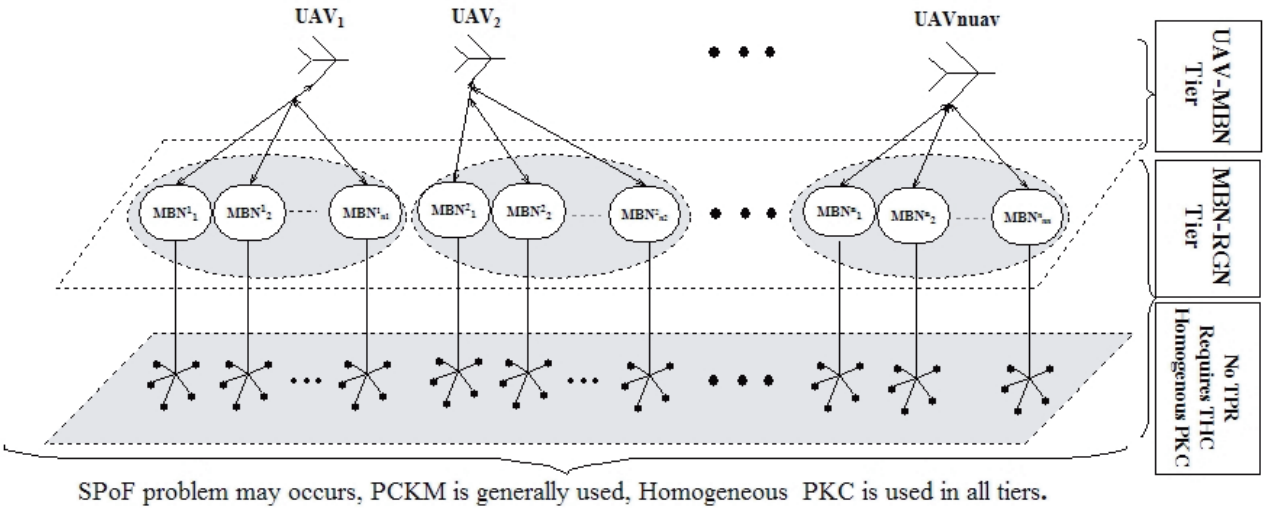

Figure 1. Structural design of the traditional military MANETs.

3.2. Structural design of the proposed protocol

In order to solve performance and security problems of classical military MANET network structure, we propose a novel adaptive military ad-hoc network security protocol. Similar to classical UAV-MBN networks, our protocol uses hierarchical multi-tier structure to secure and scale large and dynamic military MANETs. Note that this structure is especially compatible with the naturally existing hierarchy in the military networks. In this structure, each unit in the hierarchy manages a single-theater providing secure-group communication via appropriate cryptographic methods. Each UAV sets up and controls a MBN group having terrestrial mobile units in a hierarchical way. Similarly, each MBN sets up and controls RGN groups.

One of the most important contributions of our protocol is to exploit heterogeneity principle in the MBN tier. Note that classical UAV-MBN tier having tremendous advantages over homogeneous ad-hoc networks have been created by taking into consideration of heterogeneity properties of military MANETs. Based on this approach, we apply heterogeneity principle to the MBN tier so that we can obtain advantages for both key management and cryptographic cost aspects. Note that today's modern armies have high technological and diverse land force unit options (see Section 1). This diversity allows some land force units (elite ground units) to specialize so that they can have specific hardware possibilities, which can facilitate secure communication in a large and dynamic network. As an example, in classical UAV-MBN networks, UAVs are generally assumed to be having Tamper Resistant Property (TRP) [7]. TRP can be provided by a self-destruction mechanism or a special hardware which protects content of certificates and cryptographic keys. In our protocol, utilizing specialized ground units, we use TRP in the MBN tier by dividing it into TRP type MBN1 and classical MBN type MBN2 tiers. We mention benefits of this approach in Section 6.

First tier of our protocol is the UAV-MBN1 tier. UAV-MBN1 tier consists of UAV and MBN nodes having extensive communication capabilities such as long range missile batteries and Mobile Tactical Centers (MTC).

These units have sufficient capabilities for having TRP. Mobile Theater High Altitude Area Defense (THAAD) missile unit can be an example for MBN1 type units. The THAAD is an easily transportable defensive weapon system to protect against hostile incoming threats such as tactical and theater ballistic missiles at ranges of 200 km and at altitudes up to 150 km. The THAAD system provides the upper tier of a "layered defensive shield" to protect high value strategic sites. Tactical Operation Center (TOC) can be given as an example for MTCs [36], [37]. Since MBN1 type nodes have TRP, even if they are captured by an active adversary, their cryptographic keys cannot be extracted. Dividing MBN tier into MBN1 and MBN2 tiers, we extend advantages of the tamper resistant mechanism into the MBN tier and obtain some advantages for key management structure. In our protocol, UAVs are mainly responsible for key distribution and certification processes as well as being bridge between MBN clusters for communication. Since number of MBN1 type nodes is limited, both storage and computational workload of UAVs are negligible.

MBN1-MBN2 is the second tier of our protocol. MBN2 nodes are generally mobile units used in a classical UAV-MBN structure having high communication abilities such as tanks, trucks and armored vehicles. Note that our protocol can still function if MBN1 type nodes are not available. In this case, MBN2 type nodes will carry out duties of MBN1 type nodes using cryptographic techniques such as threshold cryptography in order to solve trust issues of certification [9]. MBN2-RGN is the third tier of our protocol. Each MBN2 controls RGNs including light weight equipped soldiers. In this tier, different from UAV-MBN1 and MBN1-MBN2 tiers, different cryptographic techniques are used according to needs of RGN nodes. Details are given in Section 4 and 6. We demonstrate structural design of our protocol and its properties in Figure 2.

4. Cryptographic techniques and security level structure of the proposed protocol

In our protocol, we use a new multi-leveled security structure including cryptographic methods which have not been used in military MANETs as far as we know.

4.1. Signcryption and ECPVSS

First, as a major cryptographic technique, we use signcryption based key exchange schemes (DKEUTS-DKEUN). Signcryption scheme is a cryptographic method that fulfills both the functions of secure encryption and digital signature, but with a cost smaller than that required by sign-then-encrypt approach [38]. Many efficient signcryption schemes and their applications for various security problems have been proposed [39]. For instance, in [14], multi-recipient signcryption scheme has been used. This scheme uses DLP (Discrete Logarithm Problem) based signcryption schemes [10], [40] based on Shortened Digital Signatures such as SDSS1-2 (Shortened Digital Signature Standard 1-2). In our protocol, we use the DKEUTS, which is based on a SDSS1 type signcryption scheme [10]. DKEUN (Direct Key Exchange Using Nonce) is similar to the DKEUTS but it uses nonce instead of timestamps to provide freshness of the message. We give a brief description of the basic signcryption scheme based on SDSS-1-2 below.

Suppose that *Alice* signcrypts message M and sends it to *Bob* and *Bob* unsigncrypts message M. The following notation is used:

Signcryption of Message M by Alice (the sender):

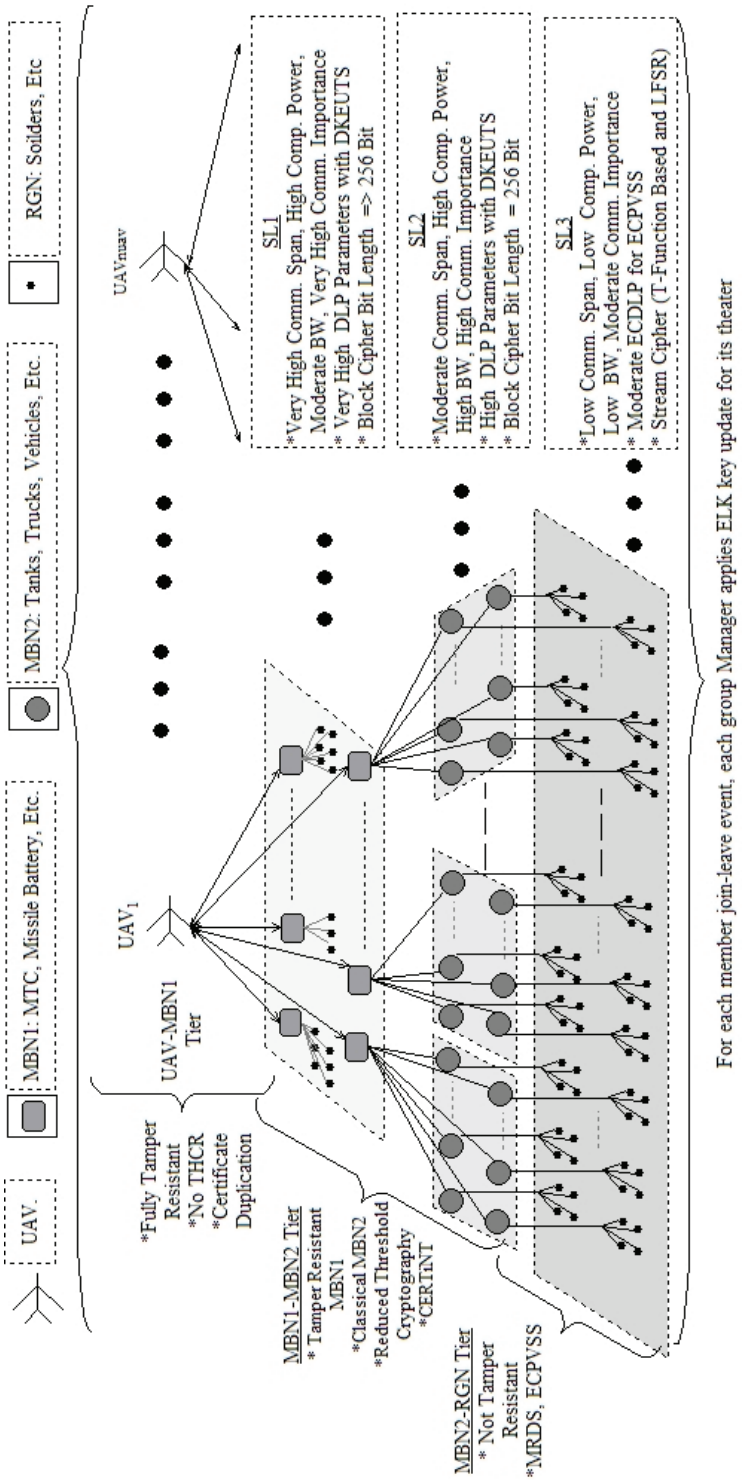

Figure 2. Structural design of the proposed protocol.

Table 1. Notation for the basic signcryption scheme.

p	Large prime number
q	A large prime factor of $p-1$
g	An integer in [1,...,$p-1$] with order $p-1$ modulo p
v_a	Private key of Alice. It is randomly chosen from [1,...,$p-1$] with $v_a \nmid (p-1)$
w_a	Public key of Alice. $w_a = g^{v_a} \bmod p$
v_b	Private key of Bob. It is randomly chosen from [1,...,$p-1$] with $v_b \nmid (p-1)$
w_b	Public key of Bob. $w_b = g^{v_b} \bmod p$

1. Alice select rc at random from [1,...,$q-1$] and computes $l' = H(w_b^{rc} \bmod p)$. Split l' into l'_1 and l'_2 of appropriate length.

2. $r = H(M, \text{bind\_info}, l'_2)$, bind_info contains data that identify the sender such as a public key certificate. l'_2 is the key of the keyed cryptographic hash function.

3. $s = rc/(r + v_a) \bmod q$ if SDSS1 is used and $s = rc/(1 + v_a \cdot r) \bmod q$ if SDSS2 is used.

4. $c = E_{l'_1}(M)$.

5. Alice sends the signcrypted text as (c, r, s) triplet to Bob.

Signcryption of (c, r, s) by Bob (the recipient):

1. Bob recovers l' from s, r, g, p, w_a, v_b :

$l' = H((w_a \cdot g^r)^{s \cdot v_b} \bmod p)$ where $s = rc/(r + x_a) \bmod q$ if SDSS1 is used and

$l' = H((w_a^r \cdot g)^{s \cdot v_b} \bmod p)$ where $s = rc/(1 + v_a \cdot r) \bmod q$ if SDSS2 is used.

2. Split l' into l'_1 and l'_2 of appropriate length.

3. $M = D_{l'_1}(c)$.

4. $r' = H(M, \text{bind\_info}, l'_2)$.

5. if $(r == r')$ then M is a valid message originated from Alice else M is not a valid message.

In addition to signcryption, we also use ECPVSS [11] to design a hybrid cryptography based key/ticket distribution mechanism. ECPVSS is a message recovery (MR) type signature scheme based on Elliptic Curve Cryptography (ECC). ECPVSS has advantages for short messages, when compared to the signature scheme with appendix [25]. ECPVSS provides confidentiality, authentication, integrity and unforgeability together as well as generating smaller signature sizes than classical digital signature algorithms. An efficient application of ECPVSS to secure satellite multicast systems can be found in TTPVSS [12].

4.2. Multi-leveled security approach

Another contribution of the proposed protocol is the use of multi-leveled security approach, in which each tier utilizes appropriate cryptographic methods according to the its specific requirement.

We suggest using a secure block cipher with appropriate modes such as Advanced Encryption Standard (AES) [41] in first and second tiers as symmetric encryption function. Note that first tier of the structure particularly requires high security (e.g., at least 256 bit block cipher). Each signcryption scheme uses cryptographic hash functions to provide integrity (e.g., at least 512 bit hash function like Secure Hash Function-512 (SHA-512)

Table 2. Notation for the proposed protocol.

$K_{i,j}^{s,d}$	Directed secret key in key exchange procedure. It is transmitted from i'^{th} source s_i to j'^{th} destination d_j.
d and s	They can be $u : UAV$, $m_1 : MBN1$ and $m_2 : MBN2$ type nodes.
$K_{i,j}^{*}$	Joint session key between i'^{th} source node and j'^{th} destination node.
γ_l	Theater level l in DBF.
$KT_i^{\gamma_l}$	Intra-theater group communication key generated by theater manager. i is index of the group manager in level l.
$su_{i,j}$	Seed value transmitted from i'^{th} theater manager to j'^{th} node in that theater. These seed values are used for moderate-time batch keying purposes.
SKG	Symmetric Key Generator. Generate keys obeying the security level, which is sent as a parameter to the SKG. Also, it may take a seed value to generate keys with related security level.
$SGNKG$	Signcryption key generator. Similar to SKG but generates signcryption related parameters.
$xa_{i,j}^{s,d}$	Signcryption private keys generated by upper tier nodes in key exchange.
$xb_{i,j}^{s,d}$	Signcryption private keys generated by lower tier nodes in key exchange.
$ya_{i,j}^{s,d}$	Signcryption public keys generated by upper tier nodes in key exchange.
$yb_{i,j}^{s,d}$	Signcryption public keys generated by lower tier nodes in key exchange.
$(c, r, s)_{i,j}^{s,d}$	Signcryption triplets.
H	Unkeyed cryptographic hash function.
$H_{K_{i,j}^{s,d}}$	Keyed cryptographic hash function.
$(E - D)_{K_{i,j}^{s,d}}$	Symmetric encryption-decryption function.
n	Number of total nodes in military MANET.
n_{type_i}	Number of *type* nodes in the i'^{th} theater in the MANET.
M	Messages.

[42], [22]). Also, the bit length of public key parameters should be as large as possible. We call security criteria chosen for the first tier as "Security level 1" (SL1). Same security approach, slightly reducing bit length of block ciphers, hash functions and public key parameters can be applied to the second tier. Note that security requirements are still high in the second tier. We call this slightly reduced security level as "Security Level 2" (SL2).

In the third tier, taking into consideration computational capabilities and communication scope of its nodes, we suggest using T-function [43], [44] combined stream ciphers such as ABC [45] or block ciphers having smaller key bit length as an alternative symmetric key cryptography method. Note that stream ciphers are especially preferred for their high speed encryption properties. Decision depends on security requirement of the third tier. Also, we use key transport protocol in this tier instead of a key exchange protocol like DKEUTS or the method presented in [13]. We call this setting "Security Level 3" (SL3).

5. Detailed description of the proposed protocol

In this section, we give detailed description of our military MANET security protocol. We first give the key management techniques used in our protocol and then present the detailed steps of our protocol.

5.1. Key management approach of our protocol

Main principle in the key management techniques of our protocol is to achieve independence of tiers, while preventing the network from performance deteriorations. Eliminating dependency between tiers allows us

to localize effect of the rekeying, thereby significantly reducing the cost of backward and forward security operations. We use ELK protocol as the main tool to perform rekeying in each tier. ELK offers computational efficiency and smaller packet sizes, when compared to some well-known protocols (e.g., LKH and OFT [28]). Whenever a node join-leave event occurs in a tier, ELK is only applied to the related parts of tier so that other parts of the network remains intact. Thus, rekeying workload of the overall network is significantly reduced. Note that our approach differs from [13] and [14] due to the structural differences. Furthermore, our key management technique adapts a batch keying mechanism [12], which suits the requirement of military MANETs.

Apart from the forward and backward security, to achieve authentication of the public keys, we also use a certification procedure. Inspired from the certification mechanism of [7], our approach deploys different cryptographic methods and key management techniques providing better coverage and flexibility. In our procedure, a certificate is given to each theater by the manager of the theater in hierarchical manner. We denote certificates as $CERT_j^{l,i}$ including $(PK_j^{l,j}, T_{\text{begin}}, T_{\text{end}}, \text{AddInf})$: Certificate of the j'^{th} unit in the l'^{th} tier and i'^{th} theater with denoted time intervals for public key $PK_j^{l,j}$. Note that inter-theater migration of nodes can be achieved by DKEUTS key exchange mechanism [34], whose details are omitted for the sake of simplicity.

5.2. Detailed description of our protocol

We adapt the DKEUTS scheme to our multi-tiered structure for UAV-MBN1 and MBN1-MBN2 tiers. In these tiers, main steps are key generation, key exchange, joint key computation, KEK transmission and secure group communication. Similar approach is also valid for the MBN2-RGN tier. However, instead of DKEUTS, ECPVSS key transport mechanism is used in this tier. Summary of notations used in our protocol is given in Table 2. Other notations are given when needed.

5.2.1. UAV-MBN1 Tier:

5.2.1.1 Key Generation:

Each UAV generates seeds of tickets, certificates and cryptographic keys for their related MBN1 type nodes. Directed symmetric keys and PKC keys required for signcryption steps are generated by UAVs obeying SL1 parameter rules. Also, public keys of each MBN1 nodes in UAV's theater are gathered. MBN1 nodes perform similar steps for both their UAV and their related MBN2 nodes.

UAVs:

$(su_{i,j}, KT_i^{\gamma_1}, K_{i,j}^{u,m_1}, x_{i,j}^{u,m_1}) = SKG(SL1)$ and UAVs obtain $y_j^{m_1,u}$ from MBN1 nodes and generate $(p_i, q_i, g_i, xa_{i,j}^{u,m_1}) = SGNKG(SL1)$.

MBN1 Nodes:

$(K_{j,i}^{m_1,u}, x_{j,i}^{m_1,u}) = SKG(SL1)$, and obtain y_i^{u,m_1} from UAVs and compute $xb_{j,i}^{m_1,u} = SGNKG(SL1)$ where $1 \leq i \leq n_u,\ 1 \leq j \leq n_{m_{1_i}}$ for each i and $l = 1, 2$.

5.2.1.2 Key Exchange Steps:

In the first step, all UAVs perform DKEUTS key transport steps by computing signcryption triplets for each of their related MBN1 nodes. Each MBN1 node verifies signcryption triplets coming from their theater

managers (UAVs) by recovering these values and checking their time-stamp together with hash value verification. Parallel to these steps, MBN1 nodes perform DKEUTS key transport and UAVs perform verification steps. At the end of key exchange steps, each UAV and each MBN1 nodes in theaters of these UAVs' obtain partial session keys $K_{i,j}^{u,m_1}$ and $K_{j,i}^{m_1,u}$.

UAVs Key Transport:

$(k_{1,i,j}^{u,m_1}, k_{2,i,j}^{u,m_1}) = H((y_i^{m_1,u})^{x_{i,j}^{u,m_1}} \bmod p_i)$ and each UAV gets their current time-stamps $TS_{i,j}^{u,m_1}$.

$c_{i,j}^{u,m_1} = E_{k_{1,i,j}^{u,m_1}}(K_{i,j}^{u,m_1}, TS_{i,j}^{u,m_1})$, $r_{i,j}^{u,m_1} = H_{k_{2,i,j}^{u,m_1}}(K_{i,j}^{u,m_1}, TS_{i,j}^{u,m_1}, CERT_j^{\gamma l,i})$,

$s_{i,j}^{u,m_1} = x_{i,j}^{u,m_1}(r_{i,j}^{u,m_1} + xa_{i,j}^{u,m_1})^{-1} \bmod q_i$ and UAVs transmit $(c_{i,j}^{u,m_1}, r_{i,j}^{u,m_1}, s_{i,j}^{u,m_1})$ tuples to MBN1 nodes.

MBN1 Nodes Verification:

$(k_{1,i,j}^{u,m_1}, k_{2,i,j}^{u,m_1}) = H((y_{i,j}^{u,m_1} \cdot g_i^{r_{i,j}^{u,m_1}})^{s_{i,j}^{u,m_1} \cdot xb_{j,i}^{m_1,u}} \bmod p_i)$ and $(K_{i,j}^{u,m_1}, TS_{i,j}^{u,m_1}) = D_{k_{1,i,j}^{u,m1}}(c_{i,j}^{u,m_1})$ then they perform the following control: If$((TS_{i,j}^{u,m_1}$ is fresh$) \wedge$ $(H_{k_{2,i,j}^{u,m_1}}(K_{i,j}^{u,m_1}, TS_{i,j}^{u,m_1}) == r_{i,j}^{u,m_1}))$ then accept, else reject.

MBN1 Nodes Key Transport:

$(k_{1,j,i}^{m_1,u}, k_{2,j,i}^{m_1,u}) = H((y_i^{u,m_1})^{x_{j,i}^{m_1,u}} \bmod p_i)$ and each MBN1 node gets their current time-stamps $TS_{j,i}^{m_1,u}$.

$c_{j,i}^{m_1,u} = E_{k_{1,j,i}^{m_1,u}}(K_{j,i}^{m_1,u}, TS_{j,i}^{m_1,u})$, $r_{j,i}^{m_1,u} = H_{k_{2,j,s}^{m_1,u}}(K_{j,i}^{m_1,u}, TS_{j,i}^{m_1,u}, CERT_j^{\gamma l,i})$,

$s_{j,i}^{m_1,u} = x_{j,i}^{m_1,u}(r_{j,i}^{m_1,u} + xa_{j,i}^{m_1,u})^{-1} \bmod q_i$ and MBN1 nodes transmit $(c_{j,i}^{m_1,u}, r_{j,i}^{m_1,u}, s_{j,i}^{m_1,u})$ tuples to UAV nodes.

UAVs Key Verification:

$(k_{1,j,i}^{m_1,u}, k_{2,j,i}^{m_1,u}) = H((y_{j,i}^{m_1,u} \cdot g_i^{r_{j,i}^{m_1,u}})^{s_{j,i}^{m_1,u} \cdot xa_{i,j}^{u,m_1}} \bmod p_i)$, and $(K_{j,i}^{m_1,u}, TS_{j,i}^{m_1,u}) = D_{k_{1,j,i}^{m_1,u}}(c_{j,i}^{m_1,u})$ then they perform the following control: If$((TS_{j,i}^{m_1,u}$ is fresh$) \wedge$ $(H_{k_{2,j,i}^{m_1,u}}(K_{j,i}^{m_1,u} TS_{j,i}^{m_1,u}) == r_{j,i}^{m_1,u}))$ then accept, else reject.

5.2.1.3 Compute Joint Keys (KEKs):

After UAVs and their MBN1 nodes obtain required session key parts, they can compute joint keys that will be used as KEKs among UAVs and MBN1 nodes. Both UAVs and MBN1 nodes perform the following operations: $K_{i,j}^* = K_{i,j}^{u,m_1} \oplus K_{j,i}^{m_1,u}$, then unique shared key pairs $K_{i,j}^*$ have been created among UAVs and MBN1 nodes. As an optional step, the following operations are performed: UAVs compute $tag_{i,j}^{u,m_1} = MAC_{K_{i,j}^*}(TS_{i,j}^{u,m_1})$ and send tags to MBN1 nodes. MBN1 nodes verify tags $if(MAC_{K_{i,j}^*}(TS_{i,j}^{u,m_1}) ==$ true).

5.2.1.4 KEK Transmission and Secure Group Communication:

UAVs prepare secure group communication keys (GK) KT_i^γ and tickets $su_{i,j}$ for their theaters. Using KEKs $K_{i,j}^*$, they send these values to MBN1 nodes. MBN1 nodes decrypt these values and using KEKs, they obtain GK. In this way, MBN1 nodes can decrypt encrypted multicast data in their theater using GK.

UAVs KEK and Encrypted Data Transmission:

$M_{i,j}^{u,m_1} = (KT_i^\gamma, su_{i,j})$, $M_{i,j}^* = E_{K_{i,j}^*}(M_{i,j}^{u,m_1})$, $M_i' = E_{KT_i^\gamma}(m_i^\gamma)$ where $M_{i,j}^{u,m_1}$ message includes intra-

theater communication keys and batch keying seeds for each nodes. For each node, $M_{i,j}^{u,m_1}$ are encrypted with shared keys $K_{i,j}^{*}$.

MBN1 Decryption:

$M_{i,j}^{u,m_1} = D_{K_{i,j}^{*}}(M_{i,j}^{*})$ and recover $KT_i^{\gamma}, su_{i,j}$ keys from $M_{i,j}^{*}$. Now, each MBN1 nodes in related theaters have intra-theater communication keys KT_i^{γ}. Using these, $m_i^{\gamma} = D_{KT_i^{\gamma}}(M_i')$ and each MBN1 nodes obtain intra-theater message m_i^{γ}. MBN1 nodes can communicate with their UAVs using $K_{i,j}^{*}$.

5.2.1.5 Member-Join Leave Events:

Whenever a MBN1 node join-leave event occurs in a UAV theater, UAV applies the ELK key update rules using $K_{i,j}^{*}$ unique keys of each MBN1 node.

5.2.2. MBN1-MBN2 Tier:

In this tier, similar to the UAV-MBN1 tier, DKEUTS is realized between MBN1 and MNB2 nodes. Key generation and parameter bit lengths obey SL2 criteria. As an optional step, MBN1 nodes can generate their directed unique keys $K_{i,j}^{m_1,m_2}$ using $su_{i,j}$ seeds. Then, each key update in MBN1-MBN2 tier can be tracked by UAVs. If this is not desired, key generation rules for these keys can be done similar to the upper tier. Due to space limitation, we give summarized version these operations. the Following notations are used: $CRS_{i,j}^{m_1,m_2}$ denotes $(c_{i,j}^{m_1,m_2}, r_{i,j}^{m_1,m_2}, s_{i,j}^{m_1,m_2})$ and $CRS_{j,i}^{m_2,m_1}$ denotes $(c_{j,i}^{m_2,m_1}, r_{j,i}^{m_2,m_1}, s_{j,i}^{m_2,m_1})$ tuples. DKEUTS parameter transport and verification procedures are represented with DTT and DTV.

Key Generation:

$K_{i,j}^{m_1,m_2} = SKG(SL2, su_{i,j})$ and UAVs $su_{i,j}$ seeds are used for key generation. Then,

$(KT_{l,i}^{\gamma}, x_{i,j}^{m_1,m_2}, x_{j,i}^{m_2,m_1}, K_{j,i}^{m_2,m_1}) = SKG(SL2)$,

$(p_i^{*}, q_i^{*}, g_i^{*}, xa_{i,j}^{m_1,m_2}, xb_{j,i}^{m_2,m_1}) = SGNKG(SL2)$ and $t^{*} = (p_i^{*}, q_i^{*}, g_i^{*})$ where $1 \leq i \leq n_{m_1},\ 1 \leq j \leq n_{m_{2_i}}$ for each i and $l = 2, 3$.

Adapted DKEUTS Steps:

Key transport and verification steps are performed by MBN1 and MBN2 nodes:

$a) CRS_{i,j}^{m_1,m_2} = DTT^{m_1,m_2}(y_{j,i}^{m_2,m_1}, TS_{i,j}^{m_1,m_2}, xa_{i,j}^{m_1,m_2}, x_{i,j}^{m_1,m_2}, t^{*})$,

$b) (TS_{i,j}^{m_1,m_2}, K_{i,j}^{m_1,m_2}) = DTV^{m_2,m_1}(y_{i,j}^{m_1,m_2}, xb_{j,i}^{m_2,m_1}, CRS_{i,j}^{m_1,m_2})$,

$c) CRS_{j,i}^{m_2,m_1} = DTT^{m_2,m_1}(y_{i,j}^{m_1,m_2}, TS_{j,i}^{m_2,m_1}, xb_{j,i}^{m_2,m_1}, x_{j,i}^{m_2,m_1}, K_{i,j}^{m_1,m_2}, t^{*})$,

$d) (TS_{j,i}^{m_2,m_1}, K_{j,i}^{m_2,m_1}) = DTV^{m_1,m_2}(y_{j,i}^{m_2,m_1}, xa_{i,j}^{m_1,m_2}, CRS_{j,i}^{m_2,m_1})$ are computed.

$K_{i,j}' = K_{i,j}^{m_1,m_2} \oplus K_{j,i}^{m_2,m_1}$ where $K_{i,j}'$ unique shared key pairs, which are computed between MBN1 and MBN2 nodes. Similar to the upper tier, $KT_i^{\gamma_2}$ intra-theater group communication key is transmitted using $K_{i,j}'$. Then, intra-theater message $m_i^{\gamma_2}$ can be securely distributed using $KT_i^{\gamma_2}$.

Member Join-Leave Events:

Whenever a MBN2 node join-leave event occurs in a MBN1 theater, the theater manager applies ELK key update rule. If the batch keying mechanism is used, theater manager generates its directed secret key using $su_{i,j}$. Then, whenever a key update occurs, instead of obtaining new key seeds from UAVs, MBN1 nodes use $su_{i,j}$ seeds to generate next seed value and inform this process to the UAV.

5.2.3. MBN2-RGN Tier:

In this tier, we suggest using SL3 criteria for key generation. As discussed in Section 4, instead of the joint key exchange, a key transport mechanism like [12] or multi-recipient signcryption scheme like [14] can be used. Particularly, KEKs and tickets are signed with ECPVSS and each RGN in MBN2 theaters obtains their KEKs. Since a key transport mechanism is used, joint key computation is not performed. Group key and bulk data are encrypted with a stream or block cipher. Considering that the most dynamic tier is MBN2-RGN tier, ticketing mechanism can be highly useful since it facilitates roaming among theaters. Also, in order to provide support to special forces and agents, special keys can be distributed to RGNs so that they can directly contact with UAVs and MBN1 nodes. Similar to other tiers, whenever a member-join leave event occurs, each MBN2 node applies ELK key update rule to the its RGN theater. Notice that, resource possibilities and security requirement of this tier are different from other tiers. Benefits of this approach are given in Section 6.

6. Analysis of the proposed military MANET security protocol

In this section, we analyze our protocol focusing on two main points. First, we analyze properties of cryptographic methods used in our protocol together with security measurement and advantages of multi-leveled security approach. Second, we give structural design and key management properties of our protocol focusing on SPoF and overall rekeying workload.

6.1. Security and performance analysis of the proposed protocol

There are three different security levels in our protocol. These security levels are created based on the following major criteria:

- Possibilities of node types in military MANET.
  - Computational and storage possibilities of nodes.
  - Bandwidth availabilities of nodes.
- Communication span of nodes.
- Importance level of communication in a theater (security requirement).
- Military rank, trust and hierarchy.
- Number of nodes and member join-leave frequency in a tier.

In order to choose secure key transmission mechanism, military rank (trust level) and capabilities of nodes are accepted as a main criteria. In UAV-MBN1 and MBN1-MBN2 tiers, since military rank and trust

level of nodes are close to each other, a joint key exchange method such as DKEUTS is preferred instead of a key transport protocol. Note that both UAV and MBN1 nodes have TRP (elite units). Also, MBN1 and MBN2 are relatively close military ranks according to ground unit military ranking. However, in the MBN2-RGN tier, military rank of MBN2 and RGN nodes are not close to each other. Thus, we suggest using a key transport mechanism like ECPVSS in this tier. In order to determine parameter bit length for the cryptographic primitives (SL level), importance level, scope of the communication and computation/bandwidth capabilities of the nodes are chosen as the selective parameters. UAVs and MBN1 type nodes such as MTCs and TOCs have large communication span. Also, since these nodes work as communication backbone and they are used for critical missions, security requirement of the UAV-MBN1 tier is determined as SL1. Note that, computational and storage possibilities of these nodes are also adequate for cryptographic operations represented in Section 5. In the MBN1-MBN2 tier, since importance level of the communication is slightly lower than the first tier, security requirement of this tier is selected as SL2. In the third tier, RGNs, which have low communication possibilities, consist of majority of the tier. Moreover, communication density is expected to be high while scope of the communication is significantly smaller than other tiers. Thus, a cryptographic algorithm focusing on high speed and low storage requirements such as ECPVSS is selected for this tier as a PKC while a stream cipher or a block cipher having smaller key bit length can be considered for symmetric encryption function.

Security analysis of our protocol is strongly related to security properties of DKEUTS, ECPVSS and their usage in our protocol. Confidentiality of bulk multicasted data in a theater is provided by symmetric encryption using the group key GK. GK is also transmitted to each theater member by GM (Group Manager) using KEKs with symmetric cryptography. Note that integrity of these messages can be provided using a MAC (Message Authentication Code). Thus, critical point is KEK transmission using hybrid cryptography. KEKs are securely distributed to theater members using signcryption based DKEUTS in first and second tiers. In order to create a secure signcryption scheme, three basic assumptions must hold: The symmetric ciphers (E-D) must hide all partial information on a message, cryptographic hash functions must behave like random function (Random Oracle) and intractability assumption of DLP must hold with appropriate parameter sizes. Under these conditions, DKEUTS and signcryption have the following properties:

- DKEUTS protocol provides confidentiality, authentication, integrity, unforgeability. Freshness of messages is provided by either time-stamps or nonces. This provides security against some active attacks. Details and proofs for these security mechanisms can be found in [38] and [46].
- Signcryption, when compared to the classical sign-then-encrypt approach, has both computational and bandwidth advantages. When compared to the sign-then encrypt approach using Shcnorr and and El Gamal signature, on average, signcryption provides 58% computational and 78% communication overhead advantages for RSA based signatures. Comparison of signcryption to Schnorr signature and El Gamal encryption for computational cost and communication overhead is demonstrated in Figure 3 [10].
- We denote cryptographic advantages of the DKEUTS protocol for both bandwidth and computational efforts as c_{sgn} and cryptographic cost of traditional methods as c_{trd}.

In MBN2-RGN tier, we use ECPVSS for secure KEK transmission. ECPVSS provides all major cryptographic services with a low cost (see Section 4.1). Figure 4 demonstrates advantages of the adaptation of

Table 3. Savings of signcryption over Sign-then-encrypt approach using Schnorr Signature and El Gamal encryption.

Security parameters $\|p\|, \|q\|$ and $\|KH(\cdot)\|$	Saving avg. comp. cost	Saving in overhead comm. overhead
768, 152, 80	58%	76%
1024, 160, 80	58%	81%
2048, 192, 96	58%	87%
4096, 256, 128	58%	91%
8192, 320, 160	58%	94%
10240, 320, 160	58%	96%

ECPVSS against some of its widely used alternatives [12]. In this comparison, bandwidth consumption of cryptographic techniques is taken as the major criterion, which is especially an important factor for bandwidth limited MBN2 and RGN nodes. In addition to this, basic cryptographic services, which are provided by related cryptographic technique, are compared. Size of the transmitted data for rekeying operation (a metric for bandwidth consumption) is measured considering total bit length requirement of associated cryptographic technique. Bit length of the session key, generated signature and certificates determine the total bit length overhead. For RSA signature [47], we assume that 1024 bit RSA signature with appendix is used. Total bit length of the message and signature is 256 bytes. Thus, total bandwidth requirement for rekeying with RSA signature is 512 bytes. DSA [48] with 1024 modulus and a common signature with appendix are also investigated. Since El Gamal encryption doubles the ciphertext [22], encrypted session key is 256 bytes and signature size of DSA for these settings is accepted as 50 bytes. Similar to El Gamal encryption, ciphertext is doubled in ECC based PKC. Thus, based upon the selection of key bit length, the encrypted session key bit length is 50–100 bytes and signature size is accepted 50 bytes. For DH and ECDH [49], common modulo sizes are the same with DSA and ECDSA. Since DH and ECDH are key exchange algorithms, two encrypted session keys are transmitted and the bit length of transmitted keys are doubled and is 256 bytes. In DH, we assume that El Gamal based cryptosystem is used for encryption while ECC based PKC algorithm is used for ECDH. Appropriate certificate sizes are selected for compared algorithms.

ECPVSS provides authentication, integrity and unforgeability while pure implementation of RSA-El Gamal, EC, DH and ECDH does not provide these properties. Using properties of ECVPSS, Implicit Certification Information (ICI) is embedded into plaintext part of transmitted data for MRDS procedure. Since plaintext is cryptographically generated pseudo-random number (KEK), it already contains sufficient redundancy. As a result, ECVPSS overhead is 40–60 bytes providing 2^{-80}–2^{-160} total break resistance security for SL3 security requirements in MBN2-RGN tier. We can see that ECPVSS is at least three times efficient than the nearest competitive method for bandwidth consumption.

6.2. Structural design and key management properties

Structural design of our protocol provides advantages for security, stability and performance aspects.

- Our protocol utilizes heterogenic structure of MBN tier in modern armies and divides the MBN tier into UAV-MBN1 and MBN1-MBN2 tiers. MBN1 tier, having tamper resistant properties, facilitates certification procedures when the central manager of the theater is destroyed. Duplication of certificates of UAVs is now possible for the MBN1 tier and this approach reduces threshold cryptography requirement.

Table 4. Advantages ECPVSS-based approach compared to widely used alternatives.

Byte		RSA - Sig.		ElGamal - DSA		EC - ECDSA		DH	ECDH	**ECPVSS**
Size of the Transmitted Data for Rekeying (BW)	Session Key	128		256		50-100		256	50-100	**Included in Signature**
	Signature	128		50		50		256	100	**20**
	Certificate	256		168		60				**20**
	Total	512		474		160		512	150	**40-60**
Authentication		no	yes	no	yes	no	yes	no	no	**yes**
Integrity		no	yes	no	yes	no	yes	no	no	**yes**
Unforgeability		no	yes	no	yes	no	yes	no	no	**yes**
Confidentiality		yes								

Table 5. ORW comparison of the proposed protocol to well-known key management protocols for PCA and PDA.

	ORW	Storage Cost	SPoF Problem
LKH	$c_{trd}O(k\log_k n-1)r$	$\mathrm{O}(\log_k n\,\lvert K\rvert)$	Yes
OFT	$c_{trd}O(\log_k n)r$	$\mathrm{O}(\log_k n\,\lvert K\rvert)$	Yes
ELK	$c_{trd}O(\log_k n)\Pr(leave)r$	$\mathrm{O}(\log_k n\,\lvert K\rvert)$	Yes
Proposed Protocol	$c_{sgn}O(\log_k thr)\Pr(leave)r_{thr}^{-1}$	$\mathrm{O}(\log_k(thr)\,\lvert K\rvert)$	No
PDC	Trust problems, not suitable for military applications		No

Notice that, if needed, threshold mechanism can still be applied to the MBN2 tier.

- Main principles behind of hybrid key management techniques of our protocol are:
  - Pure decentralized structures are not suitable for naturally hierarchical and central entity based military applications.
  - Pure centralized structures cause SPoF problems. This problem becomes much severe for highly dynamic military MANETs where survivability of nodes can not be guaranteed.
  - Our protocol divides large and dynamic MANET into subgroups like decentralized approaches in order to prevent SPoF. At the same time, it uses centralized key management technique in each theater in order to provide scalability and forward-backward security. A similar approach is also used in [34].

Significant performance gain is obtained from the independent multi-ELK-theater approach. This approach minimizes rekeying workload of MANET and provides significant performance gain. We define Overall Rekeying Workload (ORW) measurement for cost of the rekeying operation. Measurement is defined according to the three main criteria: Number of join-leave events for certain time period in certain scope of the network, r_{scope}, cost of the rekeying protocol used in network, c_{protocol} (also related with number of members affected from rekeying), and cost of cryptographic methods used in the key management protocol, c_{c}. ORW can be determined approximately as $r_{\mathrm{scope}}\cdot c_{\mathrm{protocol}}\cdot c_{\mathrm{c}}$.

We compare our protocol to pure centralized approaches (PCA) using LKH, OFT and ELK in the context of their ORW measurements. In pure centralized approach, rekeying of all network components is done by only a central entity. Thus, for aforementioned protocols, number of affected nodes is represented by n, which is all nodes in the network. In our approach, for each node join-leave event, only the related theater is affected.

Thus, number of affected nodes is represented with thr where $thr << n$. Also, number of rekeying in a single theater, r_{thr}, is much smaller than rekeying of all network, r , for certain time period and $r_{thr} << r$. m denotes benefits coming from batch keying and this factor additionally reduces ORW of our protocol. k denotes branching factor of the logical key tree. $|K|$ denotes bit length of KEKs that are used in key management protocol. Detailed cost analysis of LKH, OFT and ELK protocols can be found in [24], [27]. Comparison results are summarized given in Figure 5.

Hence, our protocol offers significant advantages over the implementation of PCAs. These advantages stem from decentralized properties of our protocol and both $r_{thr} << r$ (most important gain) and $thr << n$. Thus, rekeying performance of our protocol is better than the pure implementation of these protocols. Also, in the pure centralized approach, SPoF problem occurs while this problem is minimized in our approach. When compared to the Pure Decentralized Approach (PDA), our hybrid key management approach is more appropriate for military MANETs.

7. Conclusion and future works

Providing secure and instant communication in DBF is a vital task for future combat systems, in which military MANETs play a key role. In this paper, to provide high security and performance in military MANETs, we proposed a new multi-tiered adaptive military MANET security protocol based on hybrid cryptography and signcryption. Our protocol brings novelties for structural design, cryptographic methods and use of hybrid key management techniques in military MANETS.

Structural design of our protocol differs from traditional UAV-MBN networks with MBN1-MBN2 tier, which exploits heterogeneity of MBN tier and tamper resistance property of MBN1 nodes in modern armies. This approach allows UAVs to give their centralized certification rights to MBN1 nodes. Hence, TRP type MBN1 nodes can be used for duplication of the certification, while preventing ground unit from SPoF, even without UAV support. Furthermore, the cryptographic workload resulting from threshold cryptography operations is significantly reduced in MBN1-MBN2 tier, since the certificates can be duplicated.

Our protocol uses a new multi-leveled security approach based on efficient cryptographic primitives. Exploiting the differences and needs of military units, three main security levels are proposed based on the essential security/performance metrics of military MANETs (e.g., computational power, bandwidth capacity and communication scope). This approach provides a balance security-performance trade-off according to needs of military units. Furthermore, we adapt signcryption based DKEUTS for UAV-MBN1 and MBN1-MBN2 tiers for secure KEK distribution, which provides all computational and bandwidth advantages of signcryption to our protocol for secure multicast. Note that secure bulk data multicast is performed using symmetric cryptography, while ECPVSS is used as a key transport mechanism providing bandwidth efficiency, which is especially useful for bandwidth limited MBN2/RGN nodes. To further reduce bandwidth consumption, key seeds and ticketing mechanisms are also used.

Another contribution of our protocol is multi-tiered independent ELK theater mechanism. This hybrid key management approach integrates Iolus type decentralized techniques with ELK based centralized techniques in a hierarchical and modular manner. That is, we divide military MANETs into hierarchical tiers and theaters using decentralized approach, that prevents system from SPoF. At the same time, we use ELK centralized protocol to scale large and dynamic military sub-theaters efficiently. Hence, our protocol significantly reduces the rekeying workload, while providing forward and backward security simultaneously.

Overall, our protocol achieves high security and efficiency simultaneously in large and dynamic military MANETs. In future works, we consider addressing the secure routing, which is another challenging problem in military MANETs.

Acknowledgements

This work is supported by the State Planning Organization of Turkey under "Next Generation Satellite Networks Project", and Bogaziçi University Research Affairs.

References

[1] Attila A. Yavuz, F. Alagöz, E. Anarım, HIMUTSIS: Hierarchical Multi-Tier Adaptive Ad-hoc Network Security Protocol Based on Signcryption Type Key Exchange Schemes, in Proc. of the 21th International Symposium on Computer and Information Sciences (ISCIS'06), Istanbul, Lecture Notes in Computer Science, vol. 4263, Springer-Verlag, November 2006, 434–445.

[2] Arthur K. Cebrowski, U.S. Navy, and John J. Garstka, Network-Centric warfare, its origin and future, USNI Proceedings, January 1998.

[3] Arthur K. Cebrowski, OFT at the Network-Centric warfare conference on 22 January 2004, Washington, DC.

[4] Office of Force Transformation, The implementation of network centric warfare, 5 June 2005, Washington DC.

[5] The Warfighter Information Network-Tactical (WIN-T),
URL: `http://www.globalsecurity.org/military/systems/ground/win-t.htm`

[6] D. L. Gu, G. Pei, H. Ly, M. Gerla, and X. Hong, Hierarchical routing for multi-layer Ad-hoc wireless networks with UAVs. In IEEE MILCOM, 2000.

[7] J. Kong, H. Luo, K. Xu, D. Lihui Gu, M. Gerla, and S. Lu, Adaptive security for Multi-layer Ad Hoc networks, Wireless Communications and Mobile Computing, Special Issue on Mobile Ad Hoc Networking, vol. 2, pp. 533–547, 2002.

[8] N. Asokan and P. Ginzboorg, Key agreement in Ad-hoc networks, in Computer Communications, 23(18), pp. 1627–1637, 2000.

[9] L. Zhou and Z. Hass, Securing ad hoc networks, IEEE Network, 13(6), pages 24–30, November/December 1999.

[10] Y. Zheng, Shortened digital signature, signcryption, and compact and unforgeable key agreement schemes (A contribution to IEEE P1363 Standard for Public Key Cryptography), July 1998.

[11] L. A. Pintsov and S. A. Vanstone, Postal revenue collection in the digital age, Proceedings of Financial Cryptography, FC'00, vol. 1962, Lecture Notes in Computer Science (LNCS) , pages 105–120. Springer-Verlag, 2000.

[12] A. Altay Yavuz, F. Alagöz , E. Anarım, A new satellite multicast security protocol based on elliptic curve signatures, IEEE International Conference on Information Communication Technologies (ICTTA) , April 2006, Syria.

[13] A. Altay Yavuz, F. Alagöz, E. Anarım, Three-Tiers satellite multicast security protocol based on ECMQV and IMC methods, Computer-Aided Modeling, Analysis and Design of Communication Links and Networks (CAMAD'06), April 2006, Italy.

[14] A. Altay Yavuz, F. Alagöz, E. Anarım, NAMEPS: N -Tier Satellite Multicast Security Protocol Based on Signcryption Schemes, IEEE Globecom Conference, San Francisco, November 2006.

[15] W. Diffie, M. Hellman, New directions in cryptography, IEEE Transactions on Information Theory, Vol:.22, No.6, pp. 644–654, Nov. 1976.

[16] M.Steiner, G. Tsudik, M. Waidner, Diffie-Hellman key distribution extended to groups, Proc. 3rd ACM Symp. on Computer and Communications Security, Vol. 1, pp31–37, March 1996.

[17] G. Yao, K. Ren, F. Bao, R. Deng and D. Feng, Making the key agreement protocol in mobile Ad hoc network more efficient, In Proc. of ACNS 2003, Lecture Notes in Computer Science, Vol. 2846, p343–356, 2003.

[18] D. Augot, R. Bhaskar, V. Issarny and D. Sacchetti, An efficient group key agreement protocol for Ad-hoc networks, IEEE Workshop on Trust, Security and Privacy in Ubiquitous Computing, Taormina, Italy, 2005.

[19] A. Shamir, How to share a secret, Communications of the ACM, 612–613, 1979.

[20] M. Stadler, Publicly verifiable secret sharing, In EUROCRYPT, pages 190–199, 1996.

[21] A. Altay Yavuz, F. Alagöz , E. Anarım, A new protocol for satellite multicast security, Fifth GAP. Engineering Congress, Sanliurfa, Turkey, April 2006.

[22] D. Stinson, Cryptography theory and practice, CRC Press, Inc., Third Edition, 2005.

[23] A. Altay Yavuz, Novel methods for security mechanisms and key management techniques in wireless networks based on signcryption and hybrid cryptography, MS Thesis, Boğaziçi University, 2006.

[24] D. H. S. Rafaeli, A survey of key management for secure group communications, ACM Comp. Surveys, vol. 35, no. 3, Sept 2003, pp. 309–29.

[25] A. Menezes, P. Van Oorschot and S. Vanstone, Handbook of applied cryptography, CRC press, 1996.

[26] D. Wallner, E. Harder and R. Agee, Key management for multicast: Issues and architectures, IETF, RFC2627, June 1999.

[27] D. Balenson et al, Key management for large dynamic groups: One way function trees and amortized initialization. IETF Draft, work-in progress, draft-balenson-groupkeymgmt-oft-00.txt, February 1999.

[28] A.Perrig, D.Song and J.D. Tygar, ELK: A new protocol for efficient large-group key distribution, IEEE Security and Privacy Symposium, May 2001.

[29] S. Mittra, Iolus: A framework for scalable secure multicasting, in Proceedings of the ACM SIGCOMM'97, September 1997.

[30] D. B. Johnson and D. A. Maltz, Dynamic source routing in Ad-hoc wireless networks, Imielinski and Korth, editors, Mobile Computing, volume 353. Kluwer Academic Publishers, 1996.

[31] D. L. Gu, G. Pei, H. Ly, M. Gerla, B. Zhang and X. Hong, UAV-aided intelligent routing for Ad-hoc wireless network in single-area Theater, In IEEE WCNC, pages 1220–1225, 2000.

[32] S. R. Das, C. E. Perkins and E. E. Royer, Performance comparison of two on-demand routing protocols for Ad-hoc networks, in INFOCOM, pages 3–12, 2000.

[33] J. Li, C. Blake, D. D. Couto, H. I. Lee and R. Morris, Capacity of Ad-hoc wireless networks, in MOBICOM, 2001.

[34] Rhee, Y. Park and G. Tsudik, A group key management architecture in mobile ad-hoc wireless networks, Journal Of Communication and Networks, Vol. 6, No. 2, pp. 156–162, June 2004.

[35] R. H. Stone and G. Clarke, The T-Wing: A VTOL UAV for defense and civilian applications, Flight Internationals UAV Australia conference proceedings, 8–9 February 2001, Melbourne, Australia.

[36] The THAAD (Theatre High Altitude Area Defense) URL: `http://www.army-technology.com/projects/thaad/`

[37] V. Ziegler, 4th Infantry Division Public Affairs, Tactical Operation Centers Enhance Modular Capabilities URL: `http://www.defenselink.mil/transformation/articles/2005-03/ta030405b.html`

[38] Y. Zheng, Digital signcryption or how to achieve cost(signature encryption) << cost(signature) + cost(encryption), Advances in Cryptology - Crypto'97, Lecture Notes in Computer Science, Vol. 1294, pp. 165–179, Springer-Verlag, 1997.

[39] Y. Zheng, Signcryption and its applications in efficient public key solutions, Proceedings of 1997 Information Security Workshop (ISW'97), Lecture Notes in Computer Science, vol.1397, pp.291–312, Springer-Verlag, 1998.

[40] Y. Zheng and H. Imai, Compact and unforgeable key establishment over an ATM network, Proceedings of IEEE INFOCOM'98 , pp.411–418, 29/3-3/4, 1998.

[41] NIST, Specifications for the Advanced Encryption Standard(AES), Federal Information Processing Standards Publications (FIPS PUB) 197, November 2001. U.S. Department of Commerce, N.I.S.T.

[42] NIST, Secure Hash Standard, Federal Information Processing Standards Publications(FIPS PUB) 180-2, August 26, 2002. U.S. Department of Commerce, N.I.S.T.

[43] A. Klimov and A. Shamir, New cryptographic primitives supported on multiword T-Functions, In B. Roy and W. Meier, editors, Fast Software Encryption 2004, volume 3017, Lecture Notes in Computer Science, pages 15. Springer, 2004.

[44] A. Klimov and A. Shamir, Cryptographic applications of T-functions, Selected Areas in Cryptography (SAC), 2003.

[45] V. Anashin, A. Bogdanov, I. Kizhvatov and Sandeep Kumar, ABC: A new fast exible stream cipher, version 2, 2005. available at: `http://crypto.rsuh.ru/papers/abc-spec-v2.pdf`

[46] J. Baek, R. Steinfeld and Y. Zheng, Formal proofs for the security of signcryption, Public Key Cryptography (PKC 2002), Vol. 2274, Lecture Notes in computer Science , pp. 80–98, Springer-Verlag, 2002.

[47] R. L. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communication of the ACM, 21:120–128, 1978.

[48] T. El Gamal, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Trans. Information Theory, 31, 1985, pages 13–25.

[49] Certicom Research, Standards for efficient cryptography, SEC 1: Elliptic Curve Cryptography, Version 1.0, September 20, 2000.