HIMUTSIS: Hierarchical Multi-tier Adaptive Ad-Hoc Network Security Protocol Based on Signcryption Type Key Exchange Schemes

Attila Altay Yavuz[1], Fatih Alagoz[1], and Emin Anarim[2]

[1] Bogazici University, Department of Computer Engineering,
Bebek, Istanbul 34342, Turkey
[2] Bogazici University, Department of Electrical and Electronic Engineering,
Bebek, Istanbul 80815, Turkey
{attila.yavuz, fatih.alagoz}@boun.edu.tr,
anarim@boun.edu.tr

Abstract. Mobile Ad-hoc networks (MANETs), providing infrastructure-free wireless instant communication, play important role in tactical military networks. However, providing security in tactical military MANETs, having very large and dynamic structure without infrastructure support in hostile environments, is a very difficult task. In order to address security problems in tactical military MANETs, we propose a new HIerarchical MUlti-Tier adaptive ad-hoc network security protocol based on SIgncryption type key exchange Schemes: HIMUTSIS. Our protocol makes contribution to the military MANETs in three major points: Architectural design, cryptographic methods used in military MANETs and key management techniques. Novel architectural design of HIMUTSIS facilitates certification and key management procedures, provides flexibility and reduces cryptographic workload of the military MANETs. In HIMUTSIS, as a novelty, we offer to use DKEUTS (Direct Key Exchange Using TimeStamp) protocol providing security and performance advantages when compared to some traditional cryptographic methods. Also, multi-security level approach provides adaptive solutions for each layer of the HIMUTSIS. As a key management technique, HIMUTSIS uses hybrid key management approach which reduces rekeying workload of the networks significantly while minimizing single point of failure risk of the military MANET.

1 Introduction

Mobile Ad-hoc networks (MANETs) are infrastructure-free wireless communication networks. MANETs are considered as ideal technology for instant communication networks in both military and civilian applications. Nowadays, tactical military networks are the main application area of MANETs. Tactical military networks, having critical operation environments, require very high security and performance together. Hostile environment of tactical military networks and infrastructureless-wireless characteristic of MANETs make these networks vulnerable to various attacks and compromises.

A. Levi et al. (Eds.): ISCIS 2006, LNCS 4263, pp. 434–444, 2006.

In this paper, in order to answer these challenges, we propose a new HIerarchical MUlti-Tier adaptive ad-hoc network security protocol based on SIgncryption type key exchange Schemes: HIMUTSIS. In HIMUTSIS, we make contributions to the military MANETs for three major points. These are design and security architecture, cryptographic methods used in MANETs and key management techniques.

In HIMUTSIS, we use hierarchical multi-tier architecture including novel approaches for design aspects. Two tiered UAV-MBN (Unmanned Aerial Vehicle-Mobile Backbone Networks) networks have been recently proposed for digital battlefields utilizing heterogeneous structure of military MANETs [1], [2]. In HIMUTSIS, as a novel approach, using same heterogeneity principle, we divide MBN layer into MBN1 and MNB2 layers. This approach significantly facilitates key management and certification procedures of military MANETs and reduces the threshold cryptography requirements. Particularly, when UAVs are not available in military MANETs, this architecture provides flexibilities to the traditional approaches.

Many cryptographic methods have been proposed to secure MANETs [3]. In a secure MANET, availability, confidentiality, integrity, authentication, unforgeability and non-repudiation goals must be achieved [4]. In HIMUTSIS, as a novel approach, we use signcryption type key exhange scheme DKEUTS (Direct Key Exchange Using Time Stamp) [5] as a major cryptographic method. This method achieves all aforementioned cryptographic goals together while preventing network from some of the active attacks. Also, this method provides advantages for bandwidth and computational resource usage when compared to the classical methods. Apart from these, we propose a new multi-level security approach which provides high security for each layer while preventing system overloaded due to unnecessary cryptographic workloads.

In HIMUTSIS, we use hybrid key management techniques in order to scale very large and dynamic structure of military MANETs. We adapt independency of layers principles of [6], [7] and [17] to the MANETs. This approach significantly reduces workload of the rekeying which is required to provide forward and backward security. Also, single point of failure problem is minimized using hybrid key management architecture.

2 Related Works and Background

In order to provide major cryptographic goals in Ad-hoc networks, many cryptographic methods utilizing 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 avaliable. Thus, key exchange and key establishment schemes based on Diffie-Hellman (DH) 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 [8] protocols are used. Moreover, Hybercube , Octopus and the Burmester-Desmedt protocols are used for hierarchical group key exchange [9]. In addition to these, key agreement protocols using generic password-based authenticated key exchange schemes and DH variants with extensions to the multi-party versions have been proposed in [3]. There are many other protocols using variants of these approaches [10]. Another important technique, which is frequently used in Ad-hoc network security, is the threshold cryptography. Threshold cryptography can be used to construct distributed public key management service to solve trusted certification problem. Using this approach, if some components of the system are compromised, single point of failure problem will not occur especially for certification issues. In [4], a distributed public-key management service for Ad-hoc networks has been proposed using these approaches.

Many different key management protocols have been proposed to solve various problems of key management in large and dynamic groups. Mainly, we can classify group key management protocols into three main categories: Centralized, decentralized and hybrid key management protocols [11], [12]. In centralized group key management protocols, there is only one central entity that controls whole group. No auxiliary entity (TTP) is required to perform key distribution. However, Single Point of Failure (SPoF) problems may arise. In these protocols, hierarchical approaches, which scale group size logarithmically, are generally used. LKH (Logical Key Hierarchy) [13], OFT (One-Way Function Three) [14], and ELK (Efficient Large Group Key) [15] are well-known protocols using these approaches. In decentralized group key management protocols, the large group is split into small sub-groups. Different controllers are used for each sub-group. Iolus [16] is based on this approach. Hybrid protocols integrating these two approaches can be found in [6], [7], [17]. Note that, even if [6], [7] and [17] focus on satellite multicast systems, hybrid key management techniques of these studies can be applied to any very large and dynamic network system.

3 Architectural Design of HIMUTSIS

HIMUTSIS uses hierarchical multi-tier architecture to secure and scale large and dynamic MANETs. Notice that, this architecture is especially compatible with naturally existing hierarchical structure of the military networks. HIMUTSIS utilizes generic architecture of hierarchical military MANETs such as [18] , [1], [2]. This architecture consists of UAVs (Unmanned Aerial Vehicles), MBN (Mobile Backbone Networks) and RGN (Regular Ground Nodes). Each UAV sets up and controls a MBN group having terrestrial mobile units in hierarchical manner. Also, each MBN sets up and controls RGN groups in hierarchical manner. In HIMUTSIS, we use a novel design approach and divide MBN into MBN1 and MBN2 layers having different properties and duties. HIMUTSIS utilizes existing heterogonous structure and additional possibilities of MBN nodes in modern armies. This approach provides advantages for both security and performance aspects.

UAV-MBN1 layer consist of UAVs and MBN nodes having extensive communication capabilities such as long range missile batteries and mobile tactical centers. Notice that, as a reasonable assumption, both UAVs and MBN1 type nodes have advanced tamper resistant mechanism (for UAVs, an appropriate self-destruction mechanism can be applied) [2]. Thus, even if they are destroyed or captured by enemy, they will not comprise their cryptographic keys or certificates. Dividing MBN into MBN1 and MBN2 layers, we extend advantages of tamper resistant mechanism into MBN layer and obtain some advantages for key management architecture. 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 neglible.

MBN1-MBN2 is the second layer of our protocol. MBN2 nodes are generally mobile units used in classical UAV-MBN structure having high communication abilities. Special fighting units like trucks, tanks having beam-forming antennas can offer high-speed point-to-point direct wireless links in this layer [19]. MBN1-MBN2 layer utilizes possibilities of existing heterogeneous formation in MBN layer especially for armies having specialized ground units. This approach uses same heterogeneity principle which leads the creation of UAV-MBN networks. Notice 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 specific cryptographic techniques such as threshold cryptography in order to solve trust issues of certification [4].

MBN2-RGN is the third layer of our protocol. Each MBN2 controls RGNs including light weight equipped soldiers. In this layer, cryptographic algorithms are different from other layers. Details are given in section 4 and 6.

4 Cryptographic Techniques and Security Level Architecture of HIMUTSIS

In HIMUTSIS, we use a new multi-level security architecture including cryptographic methods which have not been used in MANETs as far as our concern.

In HIMUTSIS, as a novel approach, we use signcryption based key exchange schemes as a major cryptographic method. Signcryption is a relatively new concept in cryptography. 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 [20]. Many efficient signcryption schemes and their applications for various security problems have been proposed [21]. For instance, in [17], multi-recipient signcryption scheme has been used. In HIMUTSIS, we use DKEUTS (Direct Key Exchange Protocol Using a Timestamp) based on SDSS1 type signcryption scheme [5].

In HIMUTSIS, we suggest using a secure block cipher with appropriate modes such as AES in first and second layers as symmetric encryption part of the signcryption process. Notice that, first layer of the architecture particularly requires very high security. Thus, we suggest using at least 256 bit block cipher in this layer. Each signcryption scheme uses cryptographic hash functions to provide integrity and authentication. We suggest using at least 512 bit hash function such as SHA-512 [22]. Notice that, SHA-1 has been broken and threats for hash functions are in increase. Also, bit length of public key parameters should be hold as large as possible. We call security criteria determined for first layer as "Security level 1" (SL1). Same security approach, sligthly reducing bit length of block ciphers, hash functions and public key parameters can be applied to the second layer. Notice that, security requirements are still high in second layer. We call this slightly reduced security level as "Security Level 2" (SL2).

In third layer, taking into consideration computational capabilities and communication scope of its nodes, we suggest using T-function combined stream ciphers such as ABC [23] as an alternative symmetric key cryptography method. Stream ciphers are especially preferred for their high speed encryption properties. Also, we use key transport protocol in this layer instead of key exchange protocol like DKEUTS or [7]. Bit length requirements are reduced and cryptographic methods are changed in this layer. We call this setting as "Security Level 3" (SL3).

5 Detailed Description of HIMUTSIS

Major principle behind key management techniques of HIMUTSIS is providing independency of layers while preventing MANETs from performance deterioration and security problems. In order to provide forward and backward security (rekeying problem), we utilize independency of layers and local rekeying principles for each layer of the HIMUTSIS. We use ELK protocol as a major key management protocol in each layer. ELK protocol has advantages for rekeying cost and size of the packets when compared to some well-known protocols such as LKH and OFT [15]. Whenever a node join-leave event occurs in the theaters (active regions in military operations), ELK protocol is applied only related parts of the layer and other parts of the network are not affected from modifications. This provides significant performance gain and drastically reduces rekeying workload of the overall network. Notice that, some of these approaches have been effectively used in [7] and [17]. However, in HIMUTSIS, key management techniques are modified because architectural design of [7] and [17] are completely different from HIMUTSIS and can not be applied directly. Apart from these, we also utilize batch keying mechanism of [6], [7] adapting them to the architecture and requirements of HIMUTSIS.

We use certification procedures to provide authentication for public key's of the nodes in each layer. In [2], authors proposed an certification services for UAV-MBN networks. Our approach utilizes some principles of [2] but differs for cryptographic methods and key management techniques. We adapt DKEUTS scheme to the our multi-tier hierarchical military MANET architecture. Following notations are used:

$K_{i,j}^{s,d}$:Directed secret key in key exchange procedure. It is transmitted from $i'th$ source s_i to $j'th$ destination d_j. Source or destination can be following node types, $u : UAV$, $m_1 : MBN1\ node$, $m_2 : MBN2\ node$. All other internal keys adapted from DKEUTS obey same notation rules. $KT_i^{\gamma_l}$: This is intra-theater group communication key generated by theater manager. γ_l represents theater level and index i denotes 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 security level which is send as a parameter to the function. 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 paramteres such as, p :Large prime number, q :A large prime factor for $(p-1)$, g :Generator of the group with order q modulo p and other signcryption parameters: $xa^{s,d}_{i,j}, xb^{s,d}_{i,j}$ are private parameters and $ya^{s,d}_{i,j}, yb^{s,d}_{i,h}$ are public parameters of signcryption based schemes. H :Unkeyed cryptographic hash function, $H_{K^{s,d}_{i,j}}$:Keyed cryptographic hash function, $(E-D)_{K^{s,d}_{i,j}}$:Symmetric encryption-decryption function. n, n_{type}, n_{type_i} : Number of total nodes, number of $type$ nodes and number of $type$ nodes in the $i'th$ theater in MANET, respectively. M : Messages. Other notations are given when they are needed. We represent certificates as $CERT^{l,i}_{j}$. Now, we give details of the first layer operations:

UAV-MBN1 Layer

5.2.1 Key Generation

UAVs: $(su_{i,j}, KT^{\gamma_1}_{i}, K^{u,m_1}_{i,j}, x^{u,m_1}_{i,j}) = SKG(SL1)$, obtain $y^{m_1,u}_{j}$ from MBN1 nodes and $(p_i, q_i, g_i, xa^{u,m_1}_{i,j}) = SGNKG(SL1)$.

MBN1 Nodes: $(K^{m_1,u}_{j,i}, x^{m_1,u}_{j,i}) = SKG(SL1)$, obtain y^{u,m_1}_{i} from UAVs and $xb^{m_1,u}_{j,i} = SGNKG(SL1)$ where $1 \leq i \leq n_u$, $1 \leq j \leq n_{m_{1_i}}$ for each i and $l = 1, 2$.

5.2.2 DKEUTS Steps

UAVs Key Transport: $(k^{u,m_1}_{1,i,j}, k^{u,m_1}_{2,i,j}) = H((y^{m_1,u}_{i})^{x^{u,m_1}_{i,j}} \bmod p_i)$ and each UAV gets their current time-stamps $TS^{u,m_1}_{i,j}$.

$c^{u,m_1}_{i,j} = E_{k^{u,m_1}_{1,i,j}}(K^{u,m_1}_{i,j}, TS^{u,m_1}_{i,j})$, $r^{u,m_1}_{i,j} = H_{k^{u,m_1}_{2,i,j}}(K^{u,m_1}_{i,j}, TS^{u,m_1}_{i,j}, CERT^{\gamma_{l,i}}_{j})$, $s^{u,m_1}_{i,j} = x^{u,m_1}_{i,j}(r^{u,m_1}_{i,j} + xa^{u,m_1}_{i,j})^{-1} \bmod q_i$ and UAVs transmit $(c^{u,m_1}_{i,j}, r^{u,m_1}_{i,j}, s^{u,m_1}_{i,j})$ tuples to the MBN1 nodes.

MBN1 Nodes Verification: $(k^{u,m_1}_{1,i,j}, k^{u,m_1}_{2,i,j}) = H((y^{u,m_1}_{i,j} \cdot g_i^{r^{u,m_1}_{i,j}})^{s^{u,m_1}_{i,j} \cdot xb^{m_1,u}_{j,i}} mod\, p_i)$, $(K^{u,m_1}_{i,j}, TS^{u,m_1}_{i,j}) = D_{k^{u,m_1}_{1,i,j}}(c^{u,m_1}_{i,j})$ then perform following control:

$If(Freshness(TS^{u,m_1}_{i,j} == true) \wedge (H_{k^{u,m_1}_{2,i,j}}(K^{u,m_1}_{i,j}, TS^{u,m_1}_{i,j}) == r^{u,m_1}_{i,j}))$ then accept else reject.

MBN1 Nodes Key Transport: $(k^{m_1,u}_{1,j,i}, k^{m_1,u}_{2,j,i}) = H((y^{u,m_1}_{i})^{x^{m_1,u}_{j,i}} \bmod p_i)$ and each MBN1 node gets their current time-stamps $TS^{m_1,u}_{j,i}$.

$c^{m_1,u}_{j,i} = E_{k^{m_1,u}_{1,j,i}}(K^{m_1,u}_{j,i}, TS^{m_1,u}_{j,i})$, $r^{m_1,u}_{j,i} = H_{k^{m_1,u}_{2,j,s}}(K^{m_1,u}_{j,i}, TS^{m_1,u}_{j,i}, CERT^{\gamma_{l,i}}_{j})$, $s^{m_1,u}_{j,i} = x^{m_1,u}_{j,i}(r^{m_1,u}_{j,i} + xa^{m_1,u}_{j,i})^{-1} \bmod q_i$ and UAVs transmit $(c^{m_1,u}_{j,i}, r^{m_1,u}_{j,i}, s^{m_1,u}_{j,i})$ tuples to the MBN1 nodes.

UAVs Key Verification: $(k^{m_1,u}_{1,j,i}, k^{m_1,u}_{2,j,i}) = H((y^{m_1,u}_{j,i} \cdot g_i^{r^{m_1,u}_{j,i}})^{s^{m_1,u}_{j,i} \cdot xa^{u,m_1}_{i,j}} mod\ p_i)$, $(K^{m_1,u}_{j,i}, TS^{m_1,u}_{j,i}) = D_{k^{m_1,u}_{1,j,i}}(c^{m_1,u}_{j,i})$ then perform following control:

$If(Freshness(TS^{m_1,u}_{j,i} == true) \wedge (H_{k^{m_1,u}_{2,j,i}}(K^{u,m_1}_{i,j}, K^{m_1,u}_{j,i} TS^{m_1,u}_{j,i}) == r^{m_1,u}_{j,i}))$ then accept else reject.

5.2.3 Complete Key Exchange

Both UAVs and MBN1 nodes: $K^{*}_{i,j} = K^{u,m_1}_{i,j} \oplus K^{m_1,u}_{j,i}$ then unique shared key pairs $K^{*}_{i,j}$ have been created among UAVs and MBN1 nodes. As an optional step: *UAV:* $tag^{u,m_1}_{i,j} = MAC_{K^{*}_{i,j}}(TS^{u,m_1}_{i,j})$ and send tags to the MBN1 nodes. MBN1 nodes verify tags $if(MAC_{K^{*}_{i,j}}(TS^{u,m_1}_{i,j}) == true)$.

5.2.4 Secure Communication and Key Transmission

UAVs: $M^{u,m_1}_{i,j} = (KT^{\gamma}_{i}, su_{i,j})$, $M^{*}_{i,j} = E_{K^{*}_{i,j}}(M^{u,m_1}_{i,j})$, $M_i' = E_{KT^{\gamma}_{i}}(m^{\gamma}_{i})$ where $M^{u,m_1}_{i,j}$ message includes intra-theater communication keys and batch keying seeds for each nodes. For each nodes, $M^{u,m_1}_{i,j}$ are encrypted with shared keys $K^{*}_{i,j}$.

MBN1: $M^{u,m_1}_{i,j} = D_{K^{*}_{i,j}}(M^{*}_{i,j})$ and recover $KT^{\gamma}_{i}, su_{i,j}$ keys from $M^{*}_{i,j}$. Now, each MBN1 nodes in related theaters have intra-theater communication keys KT^{γ}_{i} . Using these, , $m^{\gamma}_{i} = D_{KT^{\gamma}_{i}}(M_i')$ and each MBN1 nodes obtain intra-theater message m^{γ}_{i}. MBN1 nodes can communicate with their UAV using $K^{*}_{i,j}$.

5.2.5 Member-Join Leave

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

MBN1-MBN2 and MBN2-RGN Layers. In MBN1-MBN2 layer, similar to upper layer, DKEUTS key exchange is realized among MBN1 and MNB2 nodes. MBN1 may use same batch keying mechanisms. Key generation and parameter bit lengths obey SL2 criteria. As an optional step, MBN1 nodes can generate their directed unique keys $K^{m_1,m_2}_{i,j}$ using $su_{i,j}$ seeds. Then, each key update in MBN1-MBN2 layer can be tracked by UAVs. If this is not desired, key generation rules for these keys can be done similar to the upper layer. Due to space limitation, we can not give detailed steps of this layer. Details of mathematical transformations can be found in [24]. Important difference of this layer from classical architectures is minimizing threshold cryptograpy requirement. In MBN2-RGN layer, we suggest using SL3 criteria. As discussed in section 4, instead of joint key exchange, a key transport mechanism like [6] or multi-recipient signcryption scheme like [17] can be used. Benefits of this approach are given in section 6 and details can be found in [24].

6 Performance Analysis of HIMUTSIS

Properties of Cryptographic Methods Used in HIMUTSIS. Major cryptographic method used in our protocol is DKEUTS key exchange protocol. DKEUTS protocol is based on signcryption and it inherently utilizes all security properties of signcryption schemes. We summarize benefits of DKEUTS protocol to the some traditional cryptographic methods below:

- DKEUTS protocol provides confidentiality, authentication, integrity, unforgeability and non-repudiation. Notice that, many traditional cryptographic methods can not provide these five major cryptographic goals together. Freshness of the messages is provided by either time-stamps or nonces.

– 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, in average, signcryption provides 58% computational and 78 % communication overhead advantages for RSA based signatures [5]. We denote cryptographic advantages of the DKEUTS protocol for both bandwitdh and computational effort as c_{sgn} and cryptographic cost of traditional methods as c_{trd} .

Apart from benefits coming from DKEUTS, HIMUTSIS has a multi-security level architecture which provides many advantages when compared to the traditional approaches. In traditional approaches, generally, all components of the network are enforced to use same cryptographic methods without regarding their heterogeneous computational and storage possibilities. In HIMUTSIS, we use three different security levels having two different cryptographic approaches. In first and second layers, joint key exchange method DKEUTS has been preferred instead of key transport protocol used in [17] or [6] . The reason is that, in the first layer , trust level (military ranks and rights, possibilities and hardness of the capturing of the nodes can be criteria) and computational availability of UAV and MBN1 nodes are close to each other both of them having tamper resistant possibilities. Thus, both parties of the communication should have right to determine their unique key pairs $K^{*}_{i,j}$ in equal manner. Similarly, it is also reasonable for MBN1-MBN2 nodes to realize joint key exchange having equal rights. Security level of each layer depends on three major criteria: Communication scope, importance of the information and computational-storage possibilities of the nodes in that layer. In first layer and second layers, which have large communication scope, high information context importance and computational possibilities, nodes use very high and high security parameters in first and second layers, respectively. In third layer, RGNs, which have low communication possibilities and communication scope, nodes use stream ciphers focusing on high speed and low storage requirements. Also, since there is important possibilities and trust difference among MBN2 and RGNs, we use key transport protocol similar to [17] or [6]. Apart from these, in third layer, using a different approach, we suggest using T-function supported stream ciphers [23].

Architectural Design and Key Management Properties of HIMUTSIS. Architectural desing of HIMUTSIS provides advantages for security, scabilitiy and performance aspects.HIMUTSIS utilizes heterogenic structure of MBN layer and divides MBN layer into MBN1 and MBN2 layers. MBN1, having tamper resistant properties, facilitates certification procedures when central manager of the theater is destroyed. Duplication of the certificates of the UAVs is now possible for MBN1 layer and this approach reduces threshold cryptography requirement. Main principles behind of the hybrid key management techniques of the HIMUTSIS can be given as follows. Pure decentralized architectures are not suitable for naturally hierarchical and central entity based military applications. Pure centralized architectures cause SPoF problems. This problem becomes much severe for highly dynamic military MANETs where survability of nodes can not be guaranteed. HIMUTSIS divides very large and dynamic MANET into subgroups like decentralized approaches in order to prevent SPoF. At the same time, HIMUTSIS uses centralized key management technique in each theater in order to provide scalability and forward-backward security. Similar approach is also used in [18].

In HIMUTSIS, significant performance gain is obtained from independent multi-ELK-theater approach. In each theater, whenever a node join-leave event occurs, in order to provide forward and backward security, key update (rekeying) is realized on only related part of the theater using ELK and other parts of the system are not affected from these processes. This approach minimizes rekeying workload of MANET and provides significant performance gain. We define ORW (Overall Rekeying Workload) measurement for cost of the rekeying operation. Measurement is defined according to the three major criteria: Number of join-leave event 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 the cryptographic methods used in key management, c_c. ORW can be determined approximately as $r_{scope} \cdot c_{protol} \cdot c_c$.

We compare HIMUTSIS to some Pure Centralized Key Management Protocols (PCKMP) such as LKH, OFT and ELK protocols in the context of their ORW measurements. In pure centralized approach, rekeying of all network components is done by only central entity. Thus, for aforementioned protocols, number of affected nodes is represented by n, which is all nodes in the network. In HIMUTSIS, for each node join-leave, only 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 the HIMUTSIS. k denotes branching factor of the logical key tree. Detailed cost analysis of LKH, OFT and ELK protocols can be found in [11], [14]. Comparison results are given at Table 1 below.

Table 1. Comparison of HIMUTSIS with some PCKMP for ORW

	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
HIMUTSIS	$c_{sgn}O(\log_k thr) \Pr(leave) r_{thr} m^{-1}$	$\mathrm{O}(\log_k (thr) \, \lvert K \rvert)$	No
PDC	Trust problems, not suitable for military applications		No

As we have seen, HIMUTSIS has significant advantages over the pure implementation of the centralized approaches. These advantages stem from the decentralized properties of HIMUTSIS and both $r_{thr} << r$ (most important gain) and $thr << n$. Thus, performance of HIMUTSIS is better than pure implementation of these protocols. Also, in pure centralized approach, SPoF problem occurs while this problem is minimized in HIMUTSIS. When compared to Pure Decentralized Approach (PDA), HIMUTSIS is more appropriate for military MANETs as discussed above.

7 Conclusion

In this paper, we have proposed a new hierarchical multi-tiered adaptive Adhoc network security protocol based on signcryption type key establishment schemes: HIMUTSIS. HIMUTSIS brings novelties for architectural design of military MANETs, cryptographic methods used in MANETs and usage of hybrid key management approaches. Architectural design of HIMUTSIS consists of UAV, MBN1-MBN2 and RGN layers in hierarchical manner. Architectural design of HIMUTSIS differs from traditional UAV-MBN networks with MBN1-MBN2 layers utilizing heterogeneity of MBN layer and tamper resistant possibilities of MBN1 nodes. This approach makes possible to give centralized certification rights of the UAVs' to the MBN1 (tamper resistant) which reduces threshold cryptography requirement and facilitates certification procedures. HIMUTSIS uses multi-security level approach for its layers applying high security parameters with DKEUTS signcryption type key exchange in its two layers and stream ciphers based key transport schemes in the third layer. Adapted DKEUTS provides all security and computational-bandwidth advantages of signcryption schemes to the HIMUTSIS when compared to the traditional cryptography approaches. Also adapted DKEUTS prevents MANETs from some active attacks. HIMUTSIS utilizes hybrid key management techniques to the military MANETs. HIMUTSIS divides military MANETs into hierarchical layers and theaters using decentralized approach preventing system SPoF problem. In each theater, HIMUTSIS uses ELK centralized protocol to scale large and dynamic military MANETs. As a result, HIMUTSIS is especially suitable for very large and dynamic military MANETs requiring very high security and performance.

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. D. L. Gu, G. Pei, H. Ly, M. Gerla, and X. Hong. Hierarchical Routing for Multilayer Ad-hoc Wireless Networks with UAVs. In IEEE MILCOM, 2000.
2. 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.
3. N. Asokan and P. Ginzboorg. Key Agreement in Ad-hoc Networks. In Computer Communications, 23(18), pp. 1627-1637, 2000.
4. L. Zhou and Z. Hass. Securing ad hoc networks. IEEE Network, 13(6), pages 24-30, November/December 1999.

5. 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.
6. A. Altay Yavuz, F. Alagoz , E. Anarim. A new satellite multicast security protocol based on elliptic curve signatures. IEEE International Conference on Information Communication Technologies (ICTTA) , April 2006.
7. A. Altay Yavuz, F. Alagoz, E. Anarim. 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).
8. 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.
9. 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, LNCS, Vol. 2846, p343-356, 2003.
10. D. Augot and R. Bhaskar and 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.
11. 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.
12. A. Menezes, P. Van Oorschot, and S. Vanstone. Handbook of applied cryptography. CRC press, 1996.
13. D. Wallner, E. Harder, and R. Agee. Key management for multicast: Issues and architectures. IETF, RFC2627, June 1999.
14. 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.
15. 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.
16. S. Mittra. Iolus: A framework for scalable secure multicasting.In Proceedings of the ACM SIGCOMM'97, September 1997.
17. A. Altay Yavuz, F. Alagoz, E. Anarim. NAMEPS: N -Tier Satellite Multicast Security Protocol Based on Signcryption Schemes. To appear on IEEE Globecom Conference, San Francisco, 2006.
18. 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.
19. 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.
20. 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.
21. 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.
22. D. Stinson. Cryptography Theory and Practice. CRC Press, Third Edition, 2005.
23. V. Anashin , A. Bogdanov, I. Kizhvatov. ABC : A New Flexible Stream Cipher.
24. 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.