IEEE MASS Workshop on Mobile Ad-Hoc Networks for Public Safety Systems - WMAPS, Valencia, Spain, October 2011

MuSE: Novel Efficient Multi-Tier Communication Security Model for Emergency and Rescue Operations

Mohamad Sbeiti, Thang Tran, Sebastian Subik, Andreas Wolff and Christian Wietfeld
Communication Networks Institute (CNI)
Faculty of Electrical Engineering and Information Technology
Dortmund University of Technology, Germany
Email: {Mohamad.Sbeiti, Thang.Tran, Sebastian.Subik, Andreas.Wolff, Christian.Wietfeld}@tu-dortmund.de

***Abstract*—For efficient emergency process management in large scale disaster situations, fast and secure access to sensitive information of heterogeneous organizations is an indispensable goal. For this purpose, we propose a novel *Mu*lti-tier communication *S*ecurity model for *E*mergency and rescue operations (MuSE) that addresses an acceptable trade-off between performance and security of information exchange in those environments. Based on in-depth user requirements analysis, MuSE deals with the communication system upon three tiers: federation, incident network and mobile client. At the federation tier, MuSE specifies an efficient *R*ole- and *C*ertificate-based *S*ingle *S*ign *O*n solution (RC-SSO) for inter-organization communication. In contrast to its counterparts such as SAML, RC-SSO does not depend on an identity provider and reduces the SSO steps to a minimum. At the incident network tier, MuSE prescribes a *P*osition *A*ware *S*ecure and *E*fficient *R*oute discovery protocol (PASER). It aims to secure the network based on lightweight cryptography. PASER deals with the network in a hierarchical way and supports nodes positions' exchange, providing both satisfying level of security as well as an advanced network management. At the mobile client tier, MuSE restricts the network access to the rescue fighters' clients based on the lightweight standard EAP-PSK and a novel *TE*TRA-based *D*ynamic key *Di*stribution method (TEDDi).**

***Keywords*-Emergency and rescue operations; Communication security; Wireless mesh networks; Single sign on; Secure routing protocols; Authentication schemes;**

I. Introduction

The world has been recently witnessing a growing threat in terms of unprecedented attacks by different means leading towards large scale disaster and emergency situations. Recent natural and technological disasters like the tsunami in Japan (2011), the earth quake in Haiti (2010) or terrorist attacks such as the bombing at the Moscow Domodedovo Airport (2011) are a testimony of the increased vulnerability of urban and crowded areas to natural, technological and terrorist disasters.

The administrative coordination of all rescue operations and the data exchange between various involved heterogeneous organizations (e.g., fire brigades, police, real estate managements etc.) pose a major challenge since a crisis must be managed as quick as possible. Thereby, organizations and rescue fighters must cope with a huge amount of information and need to cooperate in time-critical processes. Organization-specific information systems are already available, however, these systems are mutually incompatible and can be only marginally connected [1][2]. We have addressed this challenge in [3]. A system based on an XML Protection and Rescue Markup Language (PRML) and a common data model for the information exchange between public institutions has been designed. This system enables legacy components at organization level to coexist and transparently exchange information across system boundaries. Besides, we proposed in [4] an ad hoc wireless mesh network to enable various rescue fighters to communicate anywhere anytime regardless of the environment constraints at the incident scene. Both approaches lead to synergies in the disposition of resources and the optimization of time-critical processes. Nonetheless, without a satisfactory level of security, rescue organizations lack motivation to utilize any communication system. Then, terrorists or benefiting organizations may try to disrupt the communication between rescue fighters and their Command and Control Systems (CCS) or between various CCSs. They might try to inject fraud packets to falsify CCS decisions or to access and manipulate data at organization level, where any release of such sensitive data (e.g., WikiLeaks) could cause serious troubles across countries. It is thus imperative to put in place innovative protocols and systems that not only enable the exchange of data between heterogeneous parties but also ensure a secure access to those data. Bearing in mind that the time required for exchanging these information is very crucial and can strongly influence the success of the rescue operations. Thus, one of the fundamental challenges of the communication in rescue and emergency operations is the design of a secure and efficient communication system that makes all necessary data available to efficiently manage large-scale incidents.

The rest of this paper is organized as follows: Section II reports on the communication tiers in rescue operations and reviews on their security threats. In Section III, MuSE is demonstrated and its security goals and mechanisms are discussed. Finally, in Section IV, we conclude the paper and give some outlook for future work.

II. Communication System Overview

To design an efficient and secure communication system that satisfies end user requirements, the security mechanisms applied in that system should not interfere with respect to the addressed security goals (e.g., encrypting a packet multiple times at several layers). This typically occurs when various security technologies are simply accumulated to secure the system (e.g. TLS, IPsec, WPA2), which leads to noteworthy processing delay and imposes considerable overhead on the overall performance. Therefore, a thorough study of the communication system, its security threats and

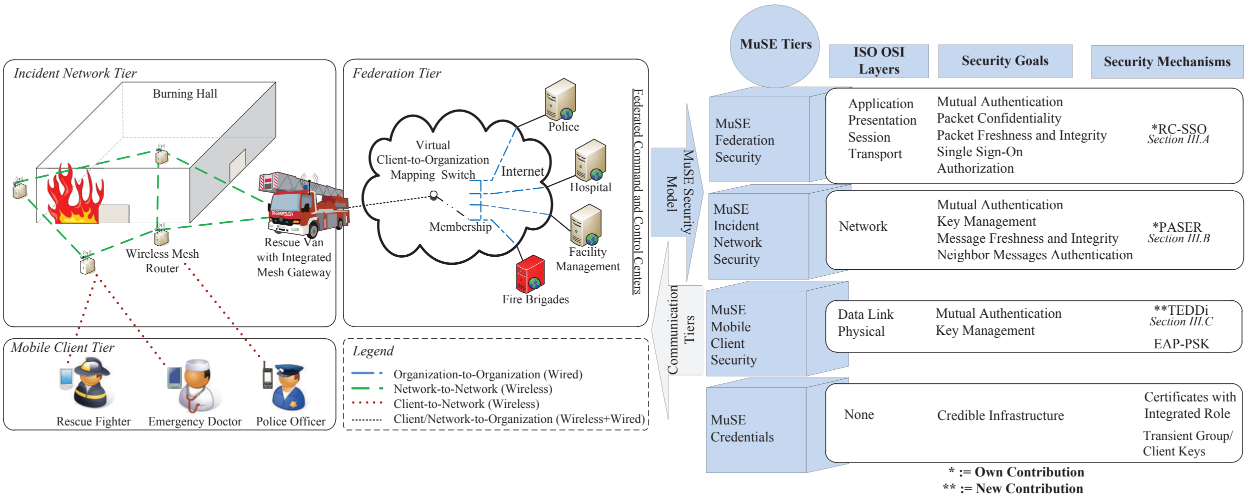

Figure 1. Rescue and emergency operations' communication tiers (left), MuSE security model (right).

the targeted security level is required before designing its security mechanisms.

A. System Tiers

Based on in-depth studies of the communication paths in emergency and rescue operations within the project SPIDER [5], we break up the communication system security of those operations into three tiers, *Federation, Incident Network* and *Mobile Client*, as depicted in Figure 1. These tiers are defined as follows:

Federation Tier: It comprises the inter communication between heterogeneous organizations as well as the communication between a client and an organization. The latter describes either the communication between a client and its organization or between that client and a partner organization. In the second case, due to jurisdiction issues, the client must use its organization as a proxy to communicate with the partner.

Incident Network Tier: It denotes the communication between the ad hoc network's mesh nodes at the incident scene. These mesh nodes typically belong to the fire brigades and are deployed on the fly during the rescue operation process.

Mobile Client Tier: Addressed is the communication between the rescue fighters' clients through the mesh nodes. Hereby, the rescue fighters might belong to different organizations such as police, Red Cross or fire brigades. Typically, firefighters are equipped with professional mobile radio devices (e.g. TETRA) because most of the communication is voice. For multimedia communication (sensor data, CCS) the officer in charge carries a WLAN device such as rugged PCs to coordinate the operations.

B. System Threats and Security Goals

With respect to the above mentioned tiers, Table I depicts the most relevant attacks and the corresponding violated security goals. It illustrates which requirements must be fulfilled in order to reach a security level that satisfies the end users.

To mitigate the risk of the attacks listed in Table I, the following security goals must be achieved:

- Entity mutual authentication
- Data confidentiality
- Data freshness and integrity
- Network neighbor transmissions authentication
- Service/network availability

We did not consider *service/network availability* by designing MuSE, because achieving this goal requires rather non cryptographic mechanisms, like frequency hopping at the incident network tier or redundant services at the federation tier, which go beyond the scope of this paper.

III. MuSE: *Mu*lti-Tier Communication *S*ecurity Model for *E*mergency Operations

MuSE is a four tier model to secure the communication in emergency and rescue operations. It disseminates the security of the system over those tiers, where each tier is composed of lightweight cryptographic primitives. In contrast to simple accumulation of security technologies and the resulting huge consumption of resources, only vital security goals are fulfilled at one tier by MuSE. Consequently, it inherits the strength and efficiency of the lightweight primitives instead of reducing it.

Thus, the main contribution of this paper is putting existing primitives together, in a sophisticated and adequate manner, to form a feasible efficient and secure communication system model for emergency and rescue operations. Figure 1 gives an overview of the MuSE tiers. We elaborate the top three tiers in details in the next subsections. The MuSE Credentials tier provides the credible infrastructure necessary for the operation of the mechanisms applied at those tiers.

A. MuSE Federation Security Tier

Nowadays, several Federated Identity Models (FIM) based on the most widely spread Security Assertion

Table I
COMMUNICATION TIERS' RELEVANT THREATS ADDRESSED BY MUSE.

Attack	**Description**	**Violated Security Goals**
	Federation Tier	
Denial-of-Service	Making organization server resources unavailable	Service availability
Eavesdropping	Revealing VoIP and data packets content	Packet confidentiality
Hijacking/Replay	Seizing control of previously established communication sessions	Packet authentication/freshness
Man-in-the-middle/Impersonation	Active eavesdropping of organization sensitive information	Mutual authentication
	Incident Network Tier	
Impersonation	Faking the identity of authorized mesh nodes (MAC or IP spoofing)	Node authentication
Denial-of-Service	Demolishing the radio signal	Network availability
Man-in-the-middle/Impersonation	Perceiving two nodes that they are talking directly to each other, when in fact the entire conversation is controlled by an attacker	Mutual authentication
Replay	Reusing valid routing messages at a later time	Message freshness
Tempering	Forging the content of routing messages generated by legitimated nodes	Message integrity
Wormhole	Tunneling routing messages via a fast transmission path controlled by two attackers, active eavesdropping of frames	Authentication of transmissions between neighboring nodes in the route discovery
	Mobile Client Tier	
Denial of Service	Flooding network with traffic, denying access to other client devices	Network availability
Eavesdropping/Data modification	Examining frames sent across the wireless medium/ flipping bits in real time; storing frames for later examination	Frame confidentiality and integrity
Man-in-the-middle/Impersonation	Masquerading legitimate nodes for network illicit use, active eavesdropping and manipulation of frames	Mutual authentication between client and network
Physical Attack	Stealing a client device and extracting the credentials	Backward and forward secrecy

Table II
RC-SSO ASSUMPTIONS.

Organizations have trustworthy certificates with integrated roles.
Roles are well defined for an effective access control.
Organization systems support SSL/TLS.

Markup Language (SAML) already exist for managing the authentication and authorization process within a closed federation. However, experimental results presented in [6] shows that SAML is not applicable for time critical applications and, therefore, is unsuitable for emergency use cases.

1) RC-SSO: Role- and Certificate-based Single Sign On System: Following the assumptions in Table II, we proposed in [7] an alternative Single Sign On solution called Role integrated Certificate-based Single Sign-On (RC-SSO) for secure and fast mobile communication between first responders at the incident scene and their distributed organizations. This solution is based on certificates with integrated roles, which reflect predefined access rights of each organization. In comparison to standard FIM approaches, RC-SSO works without an identity provider and, thereby, strongly reduces the dependency to third parties as well as the number of communication procedures. Apart from that, the role-based certificates are included in the SSL/TLS communication procedure without any modifications of this standard. Therefore, the interoperability of SSL/TLS has not been affected and no modifications at organization system level are required. Simulation and experimental results show that RC-SSO outperforms SAML by up to 80 % [7].

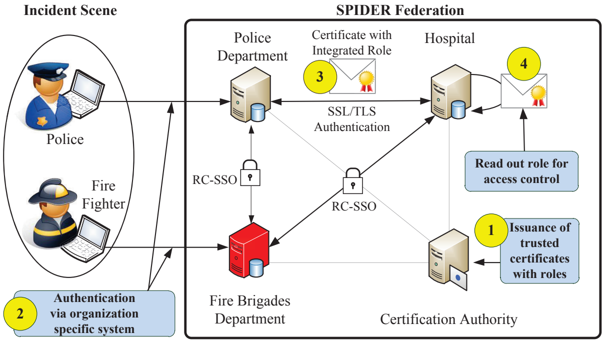

Figure 2. RC-SSO concept overview.

The main RC-SSO communication steps are illustrated based on the example in Figure 2. Noteworthy by this approach is that each organization retains its own specific system for granting access to its clients. Clients wanting to access partner services within the federation use their organization as a proxy. For instance, if a police officer wants to look for an injury at a hospital, he has to authenticate himself by the police department and call the hospital service through that department.

B. MuSE Incident Network Security Tier

In emergency and rescue operations, communication infrastructures at the incident scene, such as cellular networks, are typically demolished or down due to overload. An appropriate and common solution to deal with this issue is

Table III
PASER ASSUMPTIONS.

Only legitimated mesh nodes hold a valid certificate - these certificates are typically issued by the fire brigade organization (network operator).
Nodes feature low mobility - mesh nodes are usually relative static. Clients are rather mobile.
GPS signals are available at the application scene. Nodes incorporate a secure GPS device (secure in terms of integrity and authenticity).

the deployment of a Wireless Mesh Network (WMN).
The main characteristic of a WMN in comparison to conventional wireless networks is establishing ad hoc reliable routes between different mesh nodes from a sender to its destination. The latter makes a WMN targeted by a wide range of attacks as illustrated in Table I. To address these threats, novel security protocols need to be designed.

1) PASER: Position Aware Secure and Efficient Route Discovery: Many security solutions have been recently proposed to secure routing in MANET or WMN. However, most of them either require a lot of configuration and management [8] or comprise high computational complexity [9] or are still vulnerable to several attacks [10]. IEEE has defined in the current draft of the IEEE 802.11s standard a routing mechanism for WMN and termed it Hybrid Wireless Mesh Protocol (HWMP). However, security in routing or forwarding functionality is not specified in this standard. The protocol does not provide any authentication of routing messages. Therefore, we proposed in [11] a Position Aware Secure and Efficient Route Discovery protocol (PASER) to efficiently establish accurate routes in WMN networks in presence of external attackers. That is, based on the assumptions in Table III, PASER asserts that a communication route between mobile clients is accurate in terms of metric and legitimized mesh nodes in the presence of external attackers. PASER treats the network in a hierarchical way. It differs between gateways and mesh routers/access points. It establishes the route discovery process to a large extent upon reactive unicast messages. That is, Mesh routers/access points are always responsible, on demand, to maintain a route to the gateway. Apart from that, PASER combines digital signature with lightweight authentication tree and keyed hash function to secure the routing messages. Besides, it supports the exchange of node's geo-positions to increase the security (in particularly against wormhole attack) while enabling an advanced network management. The main building blocks of PASER are applied as follows.

Digital Signature Scheme: It is used for broadcast-messages' authentication; to establish trust between one-hop neighbors. Thus, the key pair bounded to the nodes' certificate is used for signing.

Symmetric Authentication Scheme: It is based on authentication trees [12] to authenticate unicast-messages between one-hop neighbors. Figure 3 illustrates this process:

1) Mesh node S generates random secrets. These are the leaf pre-images of the authentication tree.

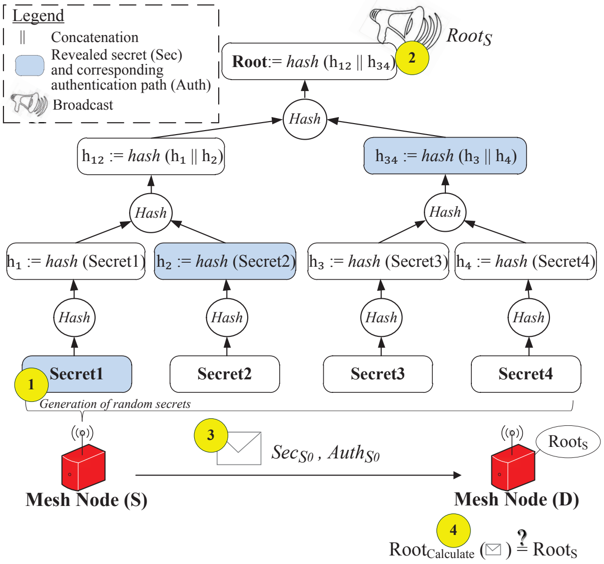

Figure 3. PASER lightweight symmetric authentication.

2) S computes the tree root and publishes it to its one-hop neighbors.
3) S, wanting to send data to mesh node D, discloses a secret and sends it along with the corresponding path with the data message to D.
4) D, already knowing Root$_S$, computes the root of the secret it has received and verifies if it matches the root of S. If true, D can trust that the message has been sent by S.

Keyed hash function: It is applied to guarantee the integrity of unicast-messages based on a secret key and to protect those messages against man-in-the-middle attacks. Theoretically, if unicast-messages were not encrypted, an external attacker might eavesdrop a secret while preventing the one-hop destination from receiving it. The attacker might then use this secret to impersonate the sender.
The key used by the hash function is the group key distributed during the setup phase of the network.

PASER's Extension: We did not consider the security of the communication between client-network or network-federation in our PASER previous work. We only focused on the network security. In this paper, since we are seeking a complete security at all tiers, we extend PASER as illustrated in Table IV.

Figure 4 depicts, with respect to security, the operations a node undergoes when it executes the new version of PASER. The example illustrates three nodes, one gateway (G), one mesh router (Y) and one mesh access point (S). These nodes join the network in the order G-Y-S, which corresponds to the steps 1, 2 and 3 respectively.

C. MuSE Mobile Client Security Tier

While frame confidentiality and integrity is guaranteed at the incident scene by the mechanisms applied at the MuSE higher tiers, the network access restriction must be ensured at the MuSE Mobile Client Security tier. An appropriate

Table IV
PASER EXTENSIONS.

Addition of a new node type: *mesh access point*. We did not distinguish between a mesh router and a mesh access point in the former version.
Distribution of transient client keys to the mesh access points. These keys are used to authenticate clients before accessing the network, and thereby restrict the network access to rescue fighters.
Integration of node's Roles, *gateway, router or AP*, in a node's certificate. Using of RC-SSO for any communication between a node and CCS.
Extending the fire brigades web services to a service that provides transient group and client keys.

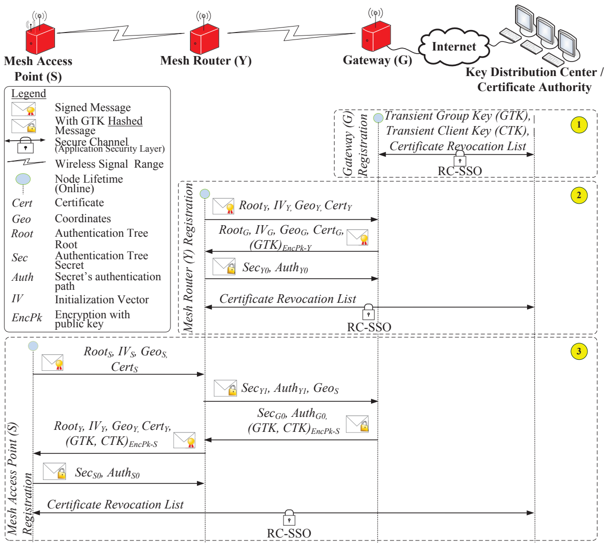
Mesh Access Point (S)
Mesh Router (Y)
Gateway (G)
Internet
Key Distribution Center / Certificate Authority
Legend
Signed Message
With GTK Hashed Message
Secure Channel (Application Security Layer)
Wireless Signal Range
Node Lifetime (Online)
Cert Certificate
Geo Coordinates
Root Authentication Tree Root
Sec Authentication Tree Secret
Auth Secret's authentication path
IV Initialization Vector
EncPk Encryption with public key
Gateway (G) Registration
Transient Group Key (GTK), Transient Client Key (CTK), Certificate Revocation List
RC-SSO
1
Mesh Router (Y) Registration
2
$Root_Y$, IV_Y, Geo_Y, $Cert_Y$
$Root_G$, IV_G, Geo_G, $Cert_G$, $(GTK)_{EncPk-Y}$
Sec_{Y0}, $Auth_{Y0}$
Certificate Revocation List
RC-SSO
Mesh Access Point (S) Registration
3
$Root_S$, IV_S, Geo_S, $Cert_S$
Sec_{Y1}, $Auth_{Y1}$, Geo_S
Sec_{G0}, $Auth_{G0}$, $(GTK, CTK)_{EncPk-S}$
$Root_Y$, IV_Y, Geo_Y, $Cert_Y$, $(GTK, CTK)_{EncPk-S}$
Sec_{S0}, $Auth_{S0}$
Certificate Revocation List
RC-SSO

Figure 4. PASER network setup process.

lightweight mechanism that deals with this issue is EAP-PSK. The latter poses, however, the challenge of distributing a transient key to the clients during each operation.
Rescue fighters typically wear gloves, which protect their hands, but hinder the input to multimedia devices via touch pad or small keypads. Furthermore, the tremendous noise at the incident scene and the usual complexity of the pre-shared-key restrict the input via speech recognition. Hence, a new concept of EAP-PSK's key provisioning is mandatory. For this purpose, we propose under the assumptions given in Table V a novel and cost-efficient, from system integration point of view, TETRA-based Dynamic key Distribution method (TEDDi).

1) TEDDi: TETRA-based Dynamic Key Distribution: In most countries rescue forces are provided with a dedicated reliable, secure and trustworthy communication system. Typical systems are trunked radio networks like TETRAPOL, Apco P25 or TETRA. In Germany the Federal Agency for Digital Radio of Security Authorities and Organizations (BDBOS) network is based on TETRA. All organizations and authorities, which are involved in public safety operations, are obligated by law to use this system for communication. During the design phase of TETRA, security and voice group communication were the main focus of the development. This led to a by far lower communication data rates in comparison to state of the art mobile network technologies (e.g., UMTS or LTE). The lack of possible data rates, however, hampers multimedia communication, which is the basis for an advanced crisis management systems. Note that in those new crisis systems, surveillance information is often enriched with video streams to support the officer in charge by analyzing the situation. As mentioned in the previous sections, the use of ad hoc networks could enable rescue forces to benefit from higher data rates, as long as a satisfying level of security can be guaranteed.

Table V
TEDDI ASSUMPTIONS.

Rescue fighters are equipped with TETRA devices or dual mode devices supporting both TETRA and WLAN.
Secure trunked radio communication system is available somewhere at the incident scene.

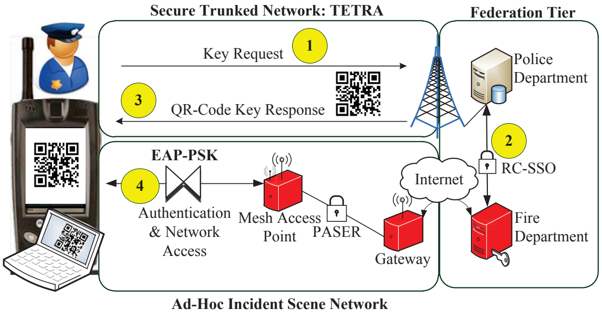

Figure 5. TEDDi application overview.

Our proposed solution, thereby, relies on the use of the TETRA network as a secure side channel to exchange security credentials via QR-codes. Those are clients' authentication and authorization information required to access the ad hoc network as well as group keys needed for secure group communication. In contrast to related approaches based on optical channels [13] or cellular networks [14], e.g., mobileTAN for online banking, the use of TETRA for out-of-band key provisioning is pragmatic since rescue fighters already use this network. Besides, this method supports hierarchical group oriented transactions enabling efficient group key management for any network used at the incident scene. The automatic interpretation of barcoded keys is well known [15] [16] and is already in use, e.g., visualTan, however, to the best of our knowledge TEDDi is the first approach that leverages the advantages of this method in public safety networks.

Figure 5 illustrates the main steps of TEDDi. First, rescue fighters, e.g., police officers request the client-network authentication key over the TETRA secured trunked network. Herewith, they request group keys required for secure group communication over the potentially non-secure WLAN channel. The key provisioning is carried out either by using the Short Data Service (SDS) or the packet data connection provided by the TETRA network. The German BDBOS network uses strong authentication mechanisms, so that an attacker cannot impersonate any party within the TETRA network (e.g., police officer). Upon receiving that request at the police department, the fire brigades' (network operator) web service responsible for the key distribution is called via RC-SSO. The latter responds with a QR-code of the keys, which is pushed back over TETRA to the corresponding rescue fighters. The network access key can be then directly used by dual-mode TETRA devices to access the network via EAP-PSK, or it can be distributed to other WLAN-only devices via an optical interface. Nowadays, smart devices are equipped with cameras and advanced software, which is able to scan QR-Codes and extract the EAP-PSK. The group keys are then used to encrypt packets among certain rescue fighters connected through the WLAN network.

IV. Conclusion and Future Work

In this paper, we propose a novel multi-tier communication security model for emergency and rescue operations (MuSE). The proposed model inherits the strength and efficiency of lightweight primitives over 4 tiers, avoiding redundant security overhead, to achieve an end users' satisfying trade-off between performance and security. At the top tier, *MuSE Federation Security*, RC-SSO enables efficient authentication and authorization of various organizations as well as confidentiality and integrity of the exchanged data. At the *MuSE Incident Network Security* tier, PASER ensures both secure network and efficient dynamic key distribution. At the *MuSE Mobile Client Security* tier, we have proposed a feasible approach, TEDDi, a novel method to dynamically distribute keys to the clients in order to access the network via EAP-PSK. The *MuSE Credentials* tier provides the credible infrastructure necessary for the operation of the before mentioned mechanisms.

In future work, we intend to capture explicitly the inherently quantitative nature of security, via a concrete or exact treatment by using practice-oriented provable security. This enables an exact assessment of the security level MuSE achieves, rather than just being secure or non-secure. Furthermore, we plan to thoroughly investigate the performance of MuSE in different scenarios, experimentally as well as in simulation, to identify its advantages and its limitations.

Acknowledgment

Our work has been conducted within the SPIDER project (Security System for Public Institutions in Disastrous Emergency scenaRios), which is part of the nationwide security research program funded by the German Federal Ministry of Education and Research (BMBF) (13N10238).

References

[1] J. Morentz, C. Doyle, L. Skelly, and N. Adam, "Unified Incident Command and Decision Support (UICDS): A Department of Homeland Security Initiative in Information Sharing," in *IEEE Conference on Technologies for Homeland Security - HST*, May 2009, pp. 182–187.

[2] D. McGarry and C. Chen, "IC.NET - Incident Command "Net": A system using EDXL-DE for intelligent message routing," in *IEEE International Conference on Technologies for Homeland Security - HST*, Nov. 2010, pp. 197–203.

[3] S. Šubik, S. Rohde, T. Weber, and C. Wietfeld, "SPIDER: Enabling Interoperable Information Sharing between Public Institutions for Efficient Disaster Recovery and Response," in *IEEE International Conference on Technologies for Homeland Security - HST*, Nov. 2010, pp. 190–196.

[4] A. Wolff, S. Šubik, and C. Wietfeld, "Performance Analysis of Highly Available Ad hoc Surveillance Networks Based on Dropped Units," in *IEEE International Conference on Technologies for Homeland Security - HST*, May 2008, pp. 123–128.

[5] (2011, Jul.) Security System for Public Institutions in Disastrous Emergency scenaRios (SPIDER). [Online]. Available: http://www.spider-federation.org

[6] T. Tran and C. Wietfeld, "Approaches for Optimizing the Performance of a Mobile SAML-based Emergency Response System," in *13th IEEE Enterprise Distributed Object Computing Conference Workshops - EDOC*, Sep. 2009, pp. 148–156.

[7] T. Tran, M. Sbeiti, and C. Wietfeld, "A novel Role- and Certificate-based Single Sign-On System for Emergency Rescue Operations," in *IEEE International Conference on Communications - ICC*, June 2011, pp. 1–6.

[8] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks," *ACM Journal on Wireless Networks*, vol. 11, no. 1-2, pp. 21–38, Jan. 2005.

[9] K. Sanzgiri, D. Laflamme, B. Dahill, B. N. Levine, C. Shields, and E. Belding-Royer, "Authenticated Routing for Ad hoc Networks," *IEEE Journal on Selected Areas in Communications*, vol. 23, pp. 598–610, Mar. 2005.

[10] L. Abusalah, A. Khokhar, and M. Guizani, "A Survey of Secure Mobile Ad hoc Routing Protocols," *IEEE Communications Surveys and Tutorials*, vol. 10, no. 4, pp. 78–93, 2008.

[11] M. Sbeiti, A. Wolff, and C. Wietfeld, "PASER: Position Aware Secure and Efficient Route Discovery for Wireless Mesh Networks," in *The Fifth International Conference on Emerging Security Information, Systems and Technologies - SECURWARE*, Aug. 2011.

[12] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1996, ch. 13, p. 556.

[13] N. C. Sherman, "Optical Out-Of-Band Key Distribution," U.S. Patent 2010/0 002 884 A1, Jan. 2010.

[14] R. Pichna, K. Lhetkangas, and K. Mustonen, "Ad hoc Networking of Terminals aided by cellular network," U.S. Patent 573 904 B2, Aug 2009.

[15] J. McCune, A. Perrig, and M. K. Reiter, "Seeing-Is-Believing: Using Camera Phones for Human-Verifiable Authentication," in *IEEE Symposium on Security and Privacy*, Berkeley/Oakland, California, USA, May 2005, pp. 110–124.

[16] G. Klyne, "Distributing public keys using 2D barcodes," United Kingdom Patent GB 2 368 755, May 2002.