A Secure Group Communication Approach for Tactical Network Environments

Filippo Poltronieri¹, Roberto Fronteddu², Cesare Stefanelli³, Niranjan Suri³,⁴, Mauro Tortonesi¹, Matthew Paulini⁴, James Milligan⁴

¹ Department of Engineering, University of Ferrara, Ferrara, Italy
{filippo.poltronieri,cesare.stefanelli,mauro.tortonesi}@unife.it
² Florida Institute for Human & Machine Cognition, Pensacola, FL, USA
{rfronteddu,n.suri}@ihmc.us
³ US Army Research Lab (ARL), Adelphi, MD, USA
niranjan.suri.civ@mail.mil
⁴ US Air Force Research Laboratory (AFRL), Rome, NY, USA
{matthew.paulini,1.james.milligan.2}@us.af.mil

Abstract—Group communication protocols that utilize multicast or local broadcast transmissions are more efficient than point-to-point protocols when disseminating the same information to multiple recipients. This is particularly true for Situation Awareness information at the tactical edge, which is transmitted from each sender to all receivers. However, group communications protocols do not address requirements for strong security mechanisms. This paper describes a novel approach that has been developed to provide secure group communications specifically to support dismounted warfighters at the tactical edge. The protocol has been incorporated into the Agile Computing Middleware’s Proactive Dissemination Service (DSPro) and supports a variety of requirements such as dynamic authorization and de-authorization of clients as well as disruption-tolerant group communications.

Keywords—group communications; security; tactical network environments; wireless networks;

I. INTRODUCTION

A tactical edge network is a complex environment composed of heterogeneous networks, often interconnected by means of link types characterized by different capabilities [1] [2]. Tactical edge networks are often deployed in scenarios where the lack of infrastructure for communications requires the adoption of Mobile Ad Hoc NETworks (MANETs). Examples could be a disaster recovery situation or a battlefield environment where opportunistic networking solutions, at both the communication infrastructure and the middleware levels, must be deployed for providing connectivity to the nodes involved in the operations.

Group communications is an essential feature for tactical edge network applications. It is required for the efficient dissemination of situation awareness information, such as Blue Force Tracking, geographical reports, traffic information, weather conditions, mission related data, and so on. On the other hand, the adoption of group communications in tactical edge networks presents many challenges. In fact, the peculiarities of these ad-hoc networks tend to invalidate the availability of the information and services and the complexity of the battlefield environment scenario requires the management of multiple groups, with different authorization and trust levels. Moreover, the use of relay nodes as bridges for different ad-hoc networks exposes the communications to data privacy and integrity issues. Finally, during battlefield operations, nodes can be compromised, and thus jeopardize the communications of the whole group.

The realization of a secure group communications solution for tactical edge networks that is able to satisfy all these requirements is a particularly challenging task. In fact, the peculiar characteristics of tactical edge networks call for dedicated secure group communication integrated within state of the art communication solutions specifically developed for that environment. Considering the restrictions that characterize tactical edge networks, secure group communications should aim to be as bandwidth efficient as possible in order to avoid overloading of an already overused channel with limited capabilities. In addition, secure group communications should be designed according to the state of the art cryptographic solutions. In fact, the modelling of ad-hoc encryption specifications could present several security flaws, both at protocol design and at the implementation level. Moreover, the dynamic nature of a battlefield environment, where nodes can be added or removed from the communication groups (e.g. de-authorized nodes) push for a solution with a low reaction time in re-establishment of valid groups. Finally, a secure group communication solution should be implemented through a peer-to-peer system capable of performing disrupt-tolerance communications in an environment that suffers from link disruptions and network partitions.

This paper presents a secure group communications solution for the Agile Computing Middleware (ACM). Our research approach focuses on the implementation of a secure group communication system for managing the authentication and authorization of nodes in a tactical environment. In particular, we propose an Authentication and Authorization (A&A) service that aims to support dismounted warfighters at the tactical edge. The design of this system takes into account key generation and updates for tackling de-authorization of nodes that are compromised in situations such as the loss of an edge device in the battlefield. The proposed solution generates group encryption keys that are independent from each other so as to avoid situations in which the compromise of key materials.
would allow a malicious node to recover the currently used encryption key. Moreover, this paper proposes a novel and secure key rotation mechanism based on multicast key dissemination for tackling the distribution of group encryption key updates at the tactical edge.

II. SCENARIO

Tactical edge networks are challenging communication environments in which connectivity could be provided by UAVs, satellites, vehicles, and dismounted soldiers as shown in Fig. 1. Because of the many link types and the ad-hoc composition of the network, limited connectivity, network partitions, and frequent disconnections present communication problems such as highly varying bandwidth and disrupted communications [1]. Tactical edge networks are common in battlefield environments and in Humanitarian Assistance and Disaster Recovery (HADR) situations, where ad-hoc networks are deployed to provide connectivity and coordinate rescue operations.

As illustrated in Fig. 1, a tactical edge network is a composition of different subsets of nodes deployed in different geographical locations. The base of operations is represented by the Tactical Operation Center (TOC), where pre-mission briefings take place and operations are coordinated through a chain of command. These operations involve the deployment of troops, such as the recon units R*, and the dismounted soldiers D*, as shown in Fig. 1, which need to coordinate and conduct their operations. For example, the commander of the dismounted platoon may need to contact the TOC to communicate an emergency situation, or the recon units could need to signal the presence of enemy troops to the platoon.

Moreover, these different subsets of nodes may not be able to communicate directly and instead have their information relayed by other nodes in order to exchange information. For instance, in Fig. 1, R1 cannot establish a direct communications link with R2, but it has to communicate via a UAV, which acts as a relay. Also, the communications between D5 and R* nodes cannot happen directly but have to pass through the TOC.

As illustrated in Fig. 1, nodes from different locations could participate in different communication groups. As a specific example, R2 and D5 are participating at the same operation and they belong to the same group, depicted as the balloon B3, while R1 just needs to communicate to the TOC forming a separate group, depicted as a B1 balloon.

One other communications issue common in battlefield scenarios is the challenge of dealing with compromised nodes. If a node has been compromised, it could invalidate the security of all the communications by injecting bogus or false data. This is the case illustrated in Fig. 1, in which the node D5 has been compromised and must be omitted from the communications group.

In addition, these links, mostly because of their precarious nature, provide poor bandwidth and intermittent connectivity, which can cause temporarily network partitions. For example, in Fig. 1, the UAV that acts as relay could lose the connection with the TOC and consequently the recon units would be momentarily unable to contact the operation center or the dismounted platoon.

Group communications is an essential feature for tackling all the situations described above on tactical edge networks. Group communications usually refers to a type of one-to-many and many-to-many communications scheme in which a single piece of information could be of interest to multiple nodes, such as dissemination of situational awareness data [3]. Group communication schemes can be realized by performing multiple retransmissions of the same information or by adopting broadcast or multicast solutions. Usually, when bandwidth efficiency is a requirement, the adoption of group communication solutions based on broadcast or multicast may be preferable to unicast based solutions. In fact, a broadcast dissemination of information could be more bandwidth efficient.

Figure 1 - A typical example of a Tactical Networking Environment
than unicast-based solution [15] and suits the broadcast capability of the radio medium well, which is most likely to be used in the deployment of ad-hoc networks.

However, the adoption of group communication techniques in tactical edge networks depends on securing these communications [4-5]. Secure communications must provide confidentiality, which ensures that a message cannot be read by unauthorized nodes and integrity, which guarantees that a message has not been forged. Furthermore, nodes should be able to exchange information only after a successful authentication procedure, which can prove the identity of the node. On the other hand, authorization ensures that specific information can be accessed only by nodes with predefined privileges. For example, nodes that belong a higher chain of command could need to exchange sensitive information, which must not be accessible to the nodes belonging to lower ranks. Finally, highly sensitive information could require the adoption of a non-repudiation mechanisms that ensures the paternity of the exchanged messages.

Implementing all these requirements in a secure group communication solution for tactical edge networks is a particularly challenging task, mostly because the dynamic nature of these environments. For instance, the presence of network partitions tends to compromise the availability of information, the ad-hoc composition could invalidate solutions for realizing centralized authentication and non-repudiation mechanisms, and the combination of these constraints undermines the integrity of the information. Implementing secure group communications for tactical edge networks requires consideration of different authorization and trust levels, adoption of strong confidentiality and integrity solutions, and addressing the possibility of compromised nodes.

In addition, in battlefield scenarios, having an awareness of the surrounding environment is essential for deployment and successful completion of operations. A good representative example of situation awareness applications is Blue Force Tracking, where all the subjects involved in the operation are interested in knowing the position and status of others. However, effective Blue Force Tracking calls for the dissemination of situation awareness information according to the nodes’ operating context (information about immediate surroundings should be disseminated) and position in the C2 chain (higher echelons should receive information about the entire battlefield, lower echelons should not). Finally, another necessary requirement of a secure group communication solution is the implementation of an efficient rekey-scheme. In fact, it is not possible for a secure group communication solution to rely on a single fixed encryption key, since its integrity could be broken for multiple reasons including outside attackers.

III. RELATED WORK

Many previous efforts have been made to develop secure group communications in MANETs, especially by exploring clustering based solutions, which are mainly based on cluster leader election for group key creation and management. Unfortunately, these solutions cannot be easily adopted in tactical edge networks. In fact, these election algorithms typically make use of a “trust all nodes policy” and perform cluster leader election mostly according to network longevity concerns (for example by assigning the leadership to the node with the highest battery level). Moreover, the process of cluster formation could require long setup times, which can decrease the group communication performance, and also a long reaction time in tackling compromised nodes. In addition, the adoption of cluster based solutions at the edge nodes could be problematic in scenarios where trust relationships between nodes are hard to achieve. Furthermore, clustering based solutions, which require signaling traffic and the creation of an overlay, could stress the capacity of the communications channel. Other research has attempted to achieve secure communications through the adoption of custom routing protocols, which are not in the scope of this paper. In fact, we want to achieve secure group communication without relying on a routing-based solution.

In [6] a group key agreement protocol based on cluster head selection is used to divide the groups into different clusters. Within each cluster, an encryption key is computed. Then, a cluster merging procedure merges all the cluster keys into a common group key, which is used for securing the communications. In [7], a Certificate Authority (CA) is used for managing the PKI of the network nodes. The generation of the group key is based on a contributory key agreement protocol, which makes use of Elliptic Curve Cryptography (ECC) and the Chinese Remainders Theorem. In [8], a fuzzy based logic is proposed for trust relationship verification during the cluster formation. When the cluster is generated, the nodes contribute to the calculation of the cluster key with a hierarchical and distributed approach. A contributory protocol is also used in [9], in which a random node, elected as Group Controller, coordinates the process of the group-key establishment. This process is composed of several node contributions and it is authenticated using Elliptic Curve Diffie Hellman (ECDH). The authors in [10] propose a two-layered approach for group key management. The nodes are divided in two main categories: Ground Nodes (GNs) and Mobile Backbone Nodes (MBNs). The MBNs act as links between different cells in which the GNs are associated. Within the same cell, the group key management is performed in a centralized fashion by the MBN node, while a contributory key management mechanism establishes a common group key between the different MBN nodes. A different solution is described in [13], which makes use of IPsec [12] and Multimedia Internet KEYing [11]. In this approach, the two protocols are used together to automatically setup an IPsec session between the devices in a multicast group communication. This approach seems promising, since it makes use of several commercial off-the-shelf components and is multicast-based. On the other hand, the deployment of this solution requires the support of a network infrastructure, which would make it challenging to adopt in tactical edge networks.

IV. AGILE COMPUTING MIDDLEWARE OVERVIEW

The Agile Computing Middleware (ACM) is a set of integrated components designed to solve the typical communication challenges of tactical edge networks. ACM provides components for realizing session mobility, reliable point-to-point communications, ad-hoc discovery services, and dissemination of information in a peer-to-peer network. Fig. 2 shows a typical composition of the solution offered by the ACM middleware in a tactical edge network.
With regards to group communication, DisService is the ACM solution for realizing peer-to-peer information dissemination in tactical edge networks. DisService realizes a peer-to-peer network in which peers can join groups and have access to information with an efficient and distributed protocol [15]. DisService acts as a group-based publish-subscribe system, in which the information is tagged to differentiate between different types of data. Examples of tagging can be Blue Force Tracking, sensor data, logistics, or other runtime information. In order to realize disruption tolerant dissemination of information, DisService uses broadcast and multicast to disseminate data and control messages over Tactical Networks. Within DisService, the transmitted data is stored and forwarded by peers, regardless of whether they are the target node, in order to reach as many peers as possible. This feature is called Opportunistic Listening [16]. The data messages contain self-describing meta-data that makes the message understandable by the peers and helps them decide whether they have to cache the data or not.

Other components of the ACM are Mockets and DSPro. Mockets is a transport protocol that provides message-oriented communication channels over tactical edge networks, while DSPro realizes Value of Information (VoI) based dissemination of information [14] on top of DisService and Mockets.

V. SECURE GROUP COMMUNICATIONS FOR ACM

This paper proposes a secure group communication approach for ACM that is specifically tailored to satisfy the requirements of tactical edge networks.

Considering the application scenario, we wanted to achieve different objectives, among them, confidentiality and integrity of the group communications. We realized an Authentication and Authorization (A&A) service, whose architecture is depicted in Fig. 3. The A&A service is designed to be run in a secure environment, such as a TOC, and has the following main components: Key Management Service (KMS), User Management Service (UMS), and Group Management Service (GMS). KMS is in charge of creating and distributing the encryption keys used to secure the group communications. GMS provides the functions for the management of multiple communication groups. UMS provides management and control functions to define which groups the users are authorized to request the shared encryption-key for. Finally, the A&A functions are accessed by tactical edge devices through the A&A Client component. In the future, we expect A&A services to also be federated, with each tactical network having its own instance. The A&A services at multiple locations will synchronize via Federation Services.

The A&A service relies on public key cryptography to ensure authentication, confidentiality, non-repudiation, and integrity in the interactions between the peers and the Key Management Service. In the envisioned architecture, the public certificate of the A&A is previously disseminated and known, while the A&A service stores the certificates of the nodes, and thus ensures the mutual authentication between the peers and the A&A service.

Once mutual authentication is established, communications are encrypted using symmetric cryptography. In addition, our secure group communications solution also guarantees data integrity and authenticity of the communications through the adoption of authenticated encryption with associated data (AEAD) encryption. Finally, combining symmetric encryption and the broadcast nature of the wireless medium enables the possibility of managing the overhead imposed by the security requirements in term of computational costs of encryption as well as bandwidth usage.

![Figure 2 - Agile Computing Middleware Overview](image-url)
The A&A service addresses the dynamic authorization and de-authorization of nodes by leveraging an encryption rekey-scheme for the group communications provided by KMS. An important property of the encryption rekey-scheme is that keys are independent of each other, which prevents malicious users from recovering new encryption keys using older encryption keys. Furthermore, this key rotation mechanism based on the key independence property allows the definition of custom polices, such as dynamically adding or excluding participants from the secure group communication.

The following subsections provide a detailed description of the complete approach. Specifically, subsection A describes the setup phase of the system for securing the group communication, B gives an explanation of the key rotation mechanism, and C describes the process of authorizing and deauthorizing new members at runtime. Finally, subsection D contains the implementation details of the secure group communication solution for ACM.

A. Initial Setup and First-Key Distribution

In the envisioned scenario, nodes go through an initial setup/configuration phase prior to deployment on a mission. This phase is similar to the process of developing and deploying a radio plan and typically occurs in a secure location, such as the Tactical Operation Center (TOC) illustrated in Fig. 1. The TOC runs on an enterprise network that is not subject to the limitations of tactical edge networks in terms of bandwidth, reliability, and latency, and vulnerability. Furthermore, being physically co-located at the TOC allows out-of-band verification about identity of users as well as devices. Assuming the TOC as the base of operations, the involved subjects can exchange information and synchronize their handheld devices during a pre-mission briefing. The first step of this synchronization process is the registration into the A&A service. In fact, UMS needs the public keys of the users/devices in order to manage the authorizations associated with the missions. In addition, the subjects need to be registered into UMS to obtain the group key for securing the mission communications. We assume the registration process to be a secure identification process since it takes place in a trusted environment. Moreover, since the security of the users’ public keys could be compromised over time (e.g. factorization attacks), we chose to limit their time validity for the duration of a single mission.

The second and final step of the synchronization process is the distribution of the initial encryption key for the mission. This step starts after the subjects have been enrolled in the A&A service, with the request of the first group key for the ongoing mission. Specifically, each enrolled user can request the encryption key for a specific group only if it has been authorized to take part in that group. Users may participate in additional groups by making a request for multiple group-keys. Each request is authenticated by KMS, which verifies the validity of the signature contained in the request message and checks whether the user requesting the group key is authorized to participate in that group.

B. Key Rotation Mechanism

In order to preserve the security of the communications, we chose to periodically rotate the encryption key used in the peer-to-peer communication channel. Even if compromising a 256-bit AES key through a brute-force attack is currently considered not computationally feasible, we must consider the event in which the encryption key is stolen or a node is identified as malicious. It is also possible that undisclosed vulnerabilities of the cipher algorithm implementation could significantly decrease the amount of time required to recover the encryption key [17]. If these vulnerabilities are unknown, an attacker could use them to exploit the security of the channel and compromise the security of the communications.

Our solution allows for rekeying and also updating the channel-key each time the group composition changes. In the developed architecture, KMS generates new group-keys that are independent from the ones generated in the past. In this way, it is not possible for a node to use a previous encryption key to recover the new one. Otherwise if the group composition is frequently changing, updating the encryption key after each join/leave could decrease the performance of the communication channel, since the encryption key update requires time and bandwidth. Considering these policies, we chose to have two different conditions that trigger a renewal of the secret key. The first one is the time validity of the group key, which can be selected as desired for each mission. The second condition is the authorization or de-authorization of a member to participate in the communication channel. In fact, the key independence property prevents a de-authorized node to decipher future communications and new members from deciphering past communications.

The key rotation mechanism is realized by KMS using a rekeying message that is disseminated to the group’s members. As illustrated in Fig. 4, the rekeying message contains multiple copies of the updated group-key, which are encrypted with each of the members’ public keys. In this way, only the intended recipients are able to decrypt and use the newly created group-key. In addition, as shown in Fig. 4, the rekeying message contains a long-term PSK that is shared by all group members and is used to encrypt the rekeying message. Moreover, a signature is attached to the rekeying message to ensure its integrity and authenticity.
contains a signature that is used to verify its authenticity. Otherwise, a possible attacker could use these public keys to generate a bogus rekeying message and control the channel. In fact, if the peer receives the bogus rekeying message and they start to use the malicious keys, the attacker will be able to sniff all the group communications or even to disseminate false or bogus messages. However, since the public key of the A&A service is known, each node can verify the authenticity of the rekeying message.

As anticipated, KMS uses the reliable multicast capabilities of DisService [15] to transmit the rekeying message in the group communication channel. Moreover, in order to address network partitioning and link disruption, we chose to not use the current channel key to further encrypt the rekeying message; instead, KMS transmits the rekeying message in the clear (but encrypted for each intended recipient). The choice of transmitting the rekeying message in the clear is crucial to our solution because any authorized node, even if it does not have the currently used group encryption key, will always be able to decrypt new keys.

Finally, we formulate the rekey message overhead as a linear function of the number of nodes n. In fact, the message contains n copies of the channel key encrypted once for each authorized node. The processing overhead of the rekey message generation also grows linearly, since its generation requires n RSA encryption operations. In addition, each node performs one decryption operation to update the group communication channel.

C. Authorization and Revocation Mechanisms

In our solution, the A&A also acts as a monitoring service. In fact, using the capabilities of DisService, it is possible to display the currently active peers in the communication channel and more importantly, to authorize new members or de-authorize existing members at runtime. The possibility of de-authorizing peers at runtime is crucial considering the scenario for the intended architecture. In military scenarios, it is not uncommon to have malicious nodes or compromised devices. To avoid these situations and preserve the security of the communications, the solution described in this paper provides specific mechanisms for authorizing and de-authorizing peers at runtime.

In the case of a new peer joining the mission, a new authorization will be granted for it and consequently, the peer will obtain the channel encryption key. The distribution of the secret key to the newly authorized member could happen in two different ways. The peer can request the mission key directly from KMS, or, if the peer is running DisService, it will receive the key rotation message containing its copy of the channel key. In fact, as explained earlier, the peer does not need the current group key in order to receive the rekeying message.

With regards to the revocation, when a member of the mission is deauthorized, a new encryption key is created and then disseminated. Since the member is no longer authorized for participating in the mission, the rekey message would not contain the deauthorized node’s copy of the encryption key. All the peers, except the deauthorized one, will change the group key to the newly created one and the deauthorized member will be de facto excluded from the communication channel.

D. Implementation details

We chose to implement the encryption and decryption layer in DisService, since it already tackles the challenges of realizing disruption tolerant group communications in tactical edge networks. The encryption layer is written in C++ and uses Advanced Encryption Standard with 256-bit keys in Galois/Counter Mode (GCM), as the encryption specification for encrypting the group communications. AES-GCM implements AEAD, which provides confidentiality and data integrity by verifying a plaintext header included in the message. It is in fact possible to verify the data authenticity of the ciphertext using the authentication tag, a sequence of bytes produced as result of the GCM encryption. Our solution also supports AES in Cipher Block Chaining (CBC) mode with random initialization vectors. We, however, prefer the GCM modality since it also provides data authenticity and integrity. Specifically, the layer has been implemented using the primitives provided by OpenSSL library.

\[ \text{Authorizing and Revoking Mechanisms} \]

\[ \text{Authorization and Revocation Mechanisms} \]

\[ \text{Time window traffic detail} \]

\[ \text{Figure 5 - KM overhead compared to baseline traffic} \]

\[ \text{Figure 6 - Time window traffic detail} \]
The A&A service is implemented in Java and it uses the language’s crypto library for generating the 256 bits AES keys and to manage the users’ public keys. The implemented public key cryptography relies on the RSA crypto-model with key sizes of 2048 bits. We considered the 2048-bits key length as sufficient security requirements since these keys have a limited time validity.

The peers interact with the A&A using a client that was also developed in Java, which takes care of generating the public key pairs. Moreover, the Android implementation of the A&A client uses the security features provided by the Android Key Store to securely store the key material on the Trusted Execution Environment (TEE) of the Android device (https://developer.android.com/training/articles/keystore.html). In particular, the use of the private-key is permitted only after a biometric authentication via fingerprint (or other supported means).

VI. EXPERIMENTAL RESULTS

We evaluated the proposed solution via emulation in the Anglova Scenario [18]. This scenario has been developed as part of the NATO IST-124 Research Task Group and represents a company task force operation in a fictitious area called Anglova, from which the scenario takes its name. The operation involves a battalion composed of six different companies, four mechanized with 24 nodes each, one command and artillery with 12 nodes, and finally the OPCON with only 4 nodes. One company takes its name.

The Anglova Scenario. In order to simulate realistic network traffic conditions, each node generates a Blue Force Track of 512 bytes every 5 seconds. The traffic generated by the track dissemination represent the baseline on which we evaluate the Key Management Protocol (KMP) overhead. KMS uses one node of the company for the rekeying message dissemination. The emulation starts with each node synchronized to an encryption key, which will be renewed every 120 seconds. To evaluate the KMP overhead, we collected the group communications traffic on every node of the company. Through this evaluation, we measured the cost of the KMP traffic in terms of the Blue Force Track baseline.

Fig. 5 shows the throughput in Bytes/s generated by the Blue Force Tracks and the KMP traffic dissemination during the whole scenario emulation. With regarding to the KMP traffic, we notice periodic peaks of traffic each 120 seconds ca. due to the rekey message transmissions. This traffic also contains the retransmissions due to the node synchronization. If the rekey message is not entirely received, the underline group communications protocol manages the requests for the missing data parts. As shown in Fig. 6, the traffic for the dissemination of the KM data is not significant compared to the traffic for the Blue Force Tracks. Fig. 5 shows a 100 second time window from t=450s to t=550s which provides a clearer view of the different types of traffic.

VII. CONCLUSION AND OUTGOING WORK

We presented a solution to provide secure group communications over tactical edge networks. In order to manage the authorizations and the generation of the encryption keys used in the peer-to-peer channel, we developed an A&A service for the nodes involved in the operations. To guarantee the security of the communications during the mission, we defined an ad-hoc Key Management Protocol for the dissemination of encryption key updates. The solution makes use of AES in GCM mode to provide confidentiality and integrity for the group communications.

We propose a security approach that is strictly bounded within the group communication protocol. This design choice let the security framework be as simple as possible, without relying on custom routing mechanisms or clustering processes. Furthermore, the encryption keys used to secure the group communication are independent (in fact they are randomly generated). The key independence property makes a newer encryption key not recoverable from older encryption keys. Using the key independence property, our solution provides an authorization and de-authorization mechanism, which makes it possible to dynamically add or exclude nodes from the group communication channel.

The proposed solution provides confidentiality and data integrity for the group communication data. Each authenticated member of the group communication channel can send and receive messages to the other members of the group. The overhead measured in our tests is negligible, even when compared to baseline data such as dissemination of Blue Force Tracks. Future work will entail expanding the current system, including the Key Management Scheme, to support Attribute Based Encryption policies.

REFERENCES


