# *An Adaptive Security Management Model for Emergency Networks*

Thiago Rodrigues de Oliveira[1,2], Sérgio de Oliveira[2], Daniel Fernandes Macedo[1], José Marcos Nogueira[1]

[1] Computer Science Department, Federal University of Minas Gerais
Campus Pampulha, Belo Horizonte, MG – Brazil

[2] Federal University of São João Del Rei
Campus Alto Paraopeba, Ouro Branco, MG – Brazil

thiagool@ufsj.edu.br, sergiool@ufsj.edu.br, damacedo@dcc.ufmg.br, jmarcos@dcc.ufmg.br

*Abstract* – **In disasters and emergency scenarios, due to a lack of network infrastructure, first-responders can build mobile ad hoc networks to send information and help disaster response coordination. However, the communication in these situations can suffer from long interruptions. This paper proposes a security management framework to dynamically configure or reconfigure emergency networks, in order to adapt the use of security components according to management information received by the decision-maker entities. The security management model includes the definition of security levels, the management information base, protocol messages and events. The emergency network activates the security mechanisms only when necessary, which avoid attacks effects and save resources.**

***Keywords – adaptive, emergency, management, security, DTN.***

## I. INTRODUCTION

Computer networks for emergency support can be established in situations caused by natural or man-made disasters. The utilization of wireless communication networks can facilitate the coordination of people and teams in disaster regions to overcome the communication challenge in these situations. Those networks are cheaper and faster to setup than wired networks.

Mobile devices can be used by the agents in rescue and relief operations in order to exchange data regarding the emergency. Typical components of these networks are ambulances, hospitals, transport vehicles, firemen, or other human agents acting in the disaster areas. A device without resource restrictions, named control center, will be responsible for managing the networks, and as such it can detect attacks to the emergency network.

Mobile ad hoc networks (MANETs) [10] are suitable for these kinds of scenarios since they do not require any previous infrastructure. However, they demand the establishment of end-to-end paths among mobile devices.

The end-to-end connectivity is highly susceptible to interruptions, what can be supported through the utilization of the DTN (Disruption Tolerant Networks) architecture [1]. By employing asynchronous communication, a DTN network can have best reachability than a MANET, especially in networks with sparse nodes. Each node can be considered a router in DTNs that present the following properties: communication based in aggregated asynchronous messages (bundles); operation without end-to-end paths, because the messages can be stored in nodes until the establishment of a contact; delays can be arbitrarily long; and it tolerates high error taxes.

DTN have security and privacy problems that limit their applicability. These networks have similar vulnerabilities to other wireless networks and specific characteristics, like unpredictable mobility and variable latency, make the security more challenging. Due to sporadic connectivity and high possibility of delay in message transmission, it's necessary to eliminate expired messages and to avoid information leak.

Among the attacks that networks can suffer, there are data losses, network flooding with junk messages, corruption of routing tables, falsification of acknowledgements, and fake network information such as meeting probabilities [4].

The security functions vary according to the environment and the application, although authentication and privacy are generally critic [3]. The security requirements in emergency networks depend on the situations and scenarios in that they are used. Various security components should be used according to the network objective in each situation.

This work proposes an adaptive security management model that sets up security and routing components in reaction to threats represented by intruders in emergency networks. This model includes the selection of security components, the description of the management information and the definition of security events. In autonomic way, security components were grouped in levels, which can be changed in answer to intrusion detection events. The aim is to reduce the effect of attacks and to save resources with the activation of the security services only when necessary.

## II. RELATED WORK

An architecture for emergency networks and some security requirements were proposed in [3]. According to this study, many of the existing security protocols won't work well if must operate in emergency networks.

A security model for the DTN architecture differs from traditional networks because the set of principles includes the own routers [2]. Related to security in DTN, [6] presents some preliminary ideas about key distribution and management, but it can be noticed that these are still open problems.

Typically, mobile ad hoc network solutions have been modified and there are researches about distributed security, like the use of distributed certified authorities [4]. Original solutions of the research community of DTN include the use of encryption based in identity [5], which allows the nodes to receive encrypted information with your public identifier.

## III. Network Model

Networks formed in emergency situations are heterogeneous in hardware, composed by notebooks, palmtops, cell phones and sensor nodes and various network technologies for communication among nodes. Some of the nodes are connected, while other nodes may not have connectivity. Such connections can drop at anytime, due to failures, displacements or other kinds of events.

Emergency networks allow a big variety of configurations. From the standpoint of safety, the control center is reliable, in other words, it can't be attacks target, and it doesn't present resources restrictions like other network participant nodes. Control center is origin or destination of all network management messages. Only it is considered network authorized participants to avoid negative effects of the possible intruders' inclusion.

## IV. Security Components for Emergency Networks

For interruption tolerant networks with precious connection resources, an end-to-end technique is not attractive for security, because scarce resources could be used to transport undesired messages until the destination. Thus, message authentication should be checked at every hop.

This work considers dynamic secure routing, priority selection for package replication, intrusion detection mechanisms, hop-by-hop and end-to-end cryptography, and necessary keys management approaches, such as a revocation scheme. Most interesting security solutions were organized and classified in components, according to their objective.

### *A. Dynamic secure routing*

Emergency networks are based on self-configuration, self-healing and self-optimization. The majority of routing protocols for DTN does not consider the security aspect as one of their main objectives. A simple attack consists to make some nodes discard all packages that they receive. For forwarding protocols, each discard is a lost package, because there is no copy in other nodes. The best defense in DTN against malicious packets losses is the use of multiple paths.

The notorious routing protocols for DTN were considered: *Direct Delivery, PRopHet, Epidemic, Spray and Wait* [12].

Applications that utilize emergency networks may require the definition of message priority, for example: Low, Medium, High or Urgent. The use of flags to indicate replication of bigger priority can restrict intruder's action and still indicate urgency and message's lifetime (TTL). Messages are discarded after this time expires. Messages defined as urgent have specific lifetime determined by the control center, because they lose sense if they are not delivered on time.

### *B. Intrusion detection*

Many attacks are facilitated if the intruder achieves to influence the network routing protocol, handling communication between legitimate nodes. This allows the corruption of routing tables, replication of old messages, injection of malicious messages in the network or the modification of valid message contents.

### *C. Revocation schemes*

Intrusion detection is normally followed by the revocation of the node with improper behavior. The revocation is the node exclusion from the network, disabling all its communications with its neighbors. This process must be authenticated to avoid intruders revoking authentic nodes.

### *D. Cryptographic primitives*

#### *1) Encryption*

This work considers that messages have the control center either as their source or as their destination, and other nodes in the way are used as routers. Although it isn't indicated for DTN, end-to-end cryptography can be utilized in critic situations to warrant bigger reliability in communication, through integrity verification or authentication of the source and destination nodes.

#### *2) Signature*

One of the differences of DTN is that an authenticated message using a digital signature, in principle, can be checked by any network element in the path. If the message contains sufficient information, so any node can at least verify the cryptographic exactness of the signature [4].

#### *3) Key management*

Both users and forward nodes in DTN have keys and certificates, and user certificates indicate the service class [7]. Nodes can send its packages signed with a private key, producing a digital signature for a specific bundle. Signatures allow the receivers to confirm the authenticity of the source node, the message integrity and relative rights to service class, through the use of the source node's public key.

DTN characteristics demand new approaches to make possible attend security requirements necessary for some applications. Therefore, no known key management in the literature is suitable [6].

#### *4) Cryptography based on identity*

A recent research area, mechanisms that utilize cryptography based on identity [5] provide much of the benefits of public key cryptography and reduce the overhead involved in obtainment and verifying public keys.

## V. Autonomic Decisions

Emergency networks must be self-adaptive, set up its components for the rational use of the resources. In this work, security components are configured based in events generated by intrusion detection systems. The detection of an intrusion triggers the reconfiguration of the security components. Intruders detected by the control center are revoked using authenticated messages. When the detection occurs in decentralized way, an intrusion detection event is generated and security components are activated, but the suspect node can't be revoked, because only the control center is reliable.

There were defined security levels to turn easier autonomic decisions based in received events. In each security level, some security components are turn on to protect against intruders. Thus, the network increases its security level based on the evidence of an intruder. The security level can be decreased too when the energy level is critical.

Table I shows the security levels. Centralized intrusion detection and access control are always enabled and does not appear in the table. In the *Low*, as there is no knowledge about contact probabilities, nodes use the epidemic routing protocol.

In the *Medium* level, some routers that store and retransmit messages turn on intrusion detection, and all nodes enable hop-by-hop cryptography. It increases the use of network resources and *PRopHet* routing protocol should be used.

In the *High* level, intrusion detection is extended to 20% of the routers, it changes to use the spray and wait routing protocol in binary operation. Message prioritization helps the identification of messages to be replicated, which can reduce intrusion effects like preventing false acknowledgments.

*Critical* level must be used when all hop-by-hop cryptography is turned on and intruders are still detected. All security components presented here are used and it considers that intruder nodes have access to some network keys. Thus, redundant cryptography, end-to-end and hop-by-hop, is used. It replicates only messages defined as high priority types, usually employed for communication with the control center.

When energy resources arrive at a critical level, nodes can decrease the security level to extend their lifetime. If network operated for long time with many security mechanisms, it's possible that all intruders have been detected and revoked.

TABLE I. Security levels for autonomic issues

| Level | Security components used |
|---|---|
| Low | - No intrusion detection in routers<br>- Epidemic routing protocol |
| Medium | - 10% of routers execute intrusion detection<br>- Hop-by-hop cryptography enabled<br>- PRopHet routing protocol |
| High | - 20% of routers execute intrusion detection<br>- Hop-by-hop cryptography enabled<br>- Replication of priority packages<br>- Spray and wait routing protocol |
| Critical | - All routers execute intrusion detection<br>- End-to-end and hop-by-hop cryptography enabled<br>- Replication of high priority packages<br>- Spray and wait routing protocol |

## VI. Management Model

The management model is composed of a management information base, a message exchange format, as well as events. Their configuration is dynamic, meaning that security components can be included, excluded, activated, and deactivated in operation time. Events provide information to the network, making possible the configuration and re-configuration of the components in an autonomic manner.

### A. Management Information Base (MIB)

To configure security components, a number of management objects have been defined for the MIB. The objects are organized according to their type: cryptography, data, and administration.

### B. Message definition

Control messages are used to activate or deactivate components such as intrusion detection, cryptography, routing protocols, priority messages selection for replication and others. A message indicating the presence of an intruder would put the network in an alert state.

The management model of this work also proposes the integration of wireless sensor networks to emergency networks. For this, it considers the utilization of the model proposed in [8] as well as its definitions and it uses the message format of the management protocol MannaNMP [9], which describes the provided services and messages format, thus like the management information base.

A number of management messages have been defined and listed in the following; in terms of the manager/agent model, they are of the type Set and are used to set or change values of objects, as defined in the MannaMNP protocol.

### C. Events

In the occurrence of events, nodes send report messages to the control center. These messages are used by the control center to change the configuration of the network, what can be done immediately or after some time. The defined events are the following: *Intrusion detection*, *Key revocation*, *Insertion of a new node*, *Critical energy level*.

## VII. Evaluation

In order to validate the management model presented here, simulations were realized to verify the behavior of the emergency network in each of defined security levels.

The mobile and heterogeneous network had total number of nodes varying between 30 and 120, and a static control center with a higher transmission radius. Nodes form groups that represent human agents in the disaster regions and vehicles such as ambulance, fireman or transport. Nodes move between points of interest were defined as two disaster regions, one region with hospitals and another with shelters.

A connection between two nodes exists if both are inside their respective transmission radius. The number of intruder nodes was defined as 3% of the network participants.

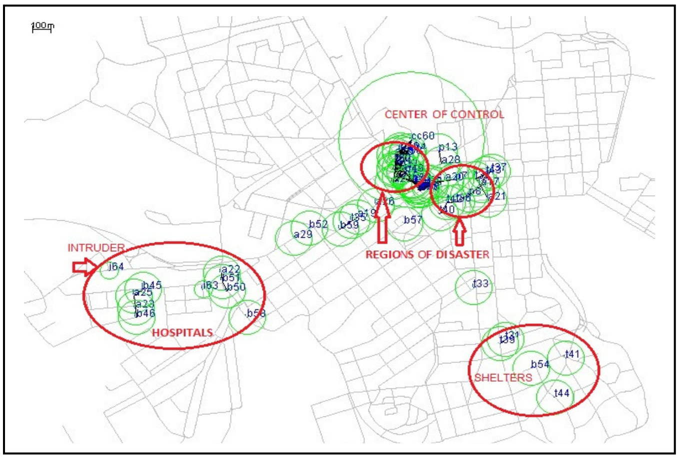


Figure 1. Simulation Scenario

As depicted in Figure 1, the motion is considered in an urban region, so the scenario utilizes a map and the nodes try to find the shortest path for their destination. With the exception of the control center, the other nodes move according with their necessities, through the simulation region that has 4500 x 3400 meters. It was performed on the "The ONE" (*Opportunistic Networking Evaluator*) simulator [11].

In each simulation, we verified the alteration of the nodes' security level and the time when it occurs, presented in the graphics below. Since all nodes start simulation in the Lower security level, this doesn't appear in Fig. 2. It can be observed that there was a change in the security level only with 60 nodes in the network. The High level was achieved with 90 participants and the Critic level with 120 nodes.

Network behavior was also verified with others intruders' percentages: 2, 3, 5 or 8% of network nodes. As percentage grows, other security levels are used and are activated faster. Fig. 3 shows that, in spite of intermittent connectivity in DTN, the propagation of messages reach all the network nodes.

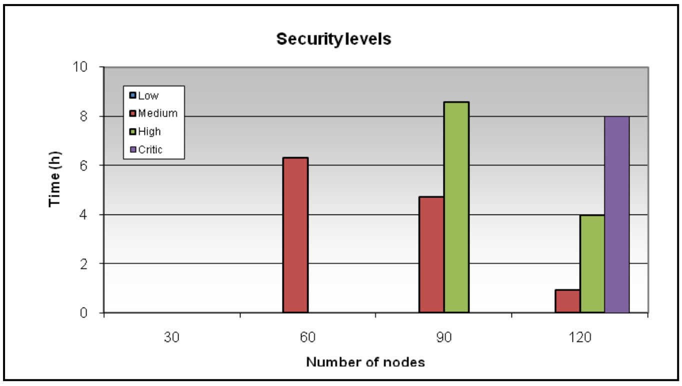
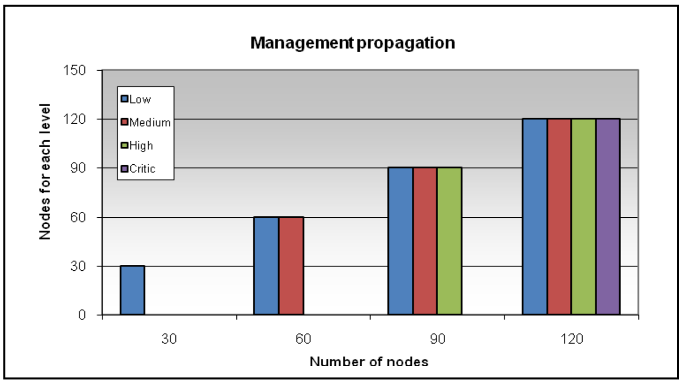


Figure 2. Time for reach security levels

Figure 3. Number of nodes for security level at each simulation finish



A security management framework, as presented here, balances network availability and resource utilization, turning the security functions on or off when necessary. It was verified that the number of management messages created is very inferior to other network messages, reaching the maximum of 3% when the Critic level is reached. Proposed security management model results in advantages independent on the number of nodes in the network, since no scenario displayed necessity to use all security components initially.

## VIII. CONCLUSION AND FUTURE WORKS

The adaptive security management presented reduces the effects of attacks and save resources, executing the proper security solutions only when necessary.

The proposed security management model employs self-management technologies. The control center can set up the security level in the nodes, turning on security components to reduce the effects of intrusions. The detection of an intrusion starts an autonomic decision to reconfigure the security levels.

Although DTN characteristics, only few messages are necessary to implement the security management, and these messages reach all the participant nodes. It is possible to save resources without a loss in network productivity while there is not an evidence of intrusions.

As future work, we propose to study which specific security solutions must be employed to secure DTN routing protocols, in order to alter the management components according to the type of attack detected in the network.

## REFERENCES

[1] Fall, K. (2004), "Messaging in difficult environments" – Intel Research Berkeley.

[2] Fall, K. (2003), "A Delay-Tolerant Network Architecture for Challenged Internets" – Intel Research Berkeley.

[3] Portmann, M. and Pirzada, A. A. (2008), "Wireless Mesh Networks for Public Safety and Crisis Management Applications" – IEEE Internet Computing.

[4] Burgess, J., Bissias, G., Corner, M. D., Levine, B. N. (2007), "Surviving Attacks on DTN without Authentication" – ACM Mobihoc.

[5] Seth, A. and Keshav, S. (2005), "Practical Security for Disconnected Nodes" – NPSEC.

[6] Symington, S. F., Farrell, S., Weiss, H. and Lovell, P. (2009), "Bundle Security Protocol Specification" – draft-irtf-dtnrg-bundle-security-08.txt.

[7] Durst, R. C. (2002), "An infrastructure security model for delay tolerant networks" – In http://www.dtnrg.org.

[8] Oliveira, S., Oliveira, T. R. and Nogueira, J. M. S. (2009), "A Policy based Security Management Architecture for Sensor Networks" – In 11th IFIP/IEEE International Symposium on Integrated Network Management.

[9] Silva, F. A., Ruiz, L. B. et al. (2005), "Defining a Wireless Sensor Network Management Protocol" – In Latin American Network Operations and Management Symposium.

[10] Zhang, Y. and Lee, W. (2000) "Intrusion detection in wireless ad-hoc networks" – In Mobile Computing and Networking, pp. 275–283.

[11] Keranen, A. and Ott, J. (2007), "Increasing reality for DTN protocol simulations." Networking Laboratory, Helsinki University of Technology, Tech. Rep.

[12] Zhang, Z. (2006). "Routing in intermittently connected mobile ad hoc networks and delay tolerant networks: overview and challenges." – In IEEE Communications Surveys & Tutorials, 8:24-37.