Requirements and System Architecture Design Consideration for First Responder Systems

Ying Huang, Wenbo He and Klara Nahrstedt
{huang23, wenbohe, klara}@cs.uiuc.edu
Department of Computer Science
University of Illinois at Urbana-Champaign

Whay C. Lee
Whay.Lee@motorola.com
Networks and Systems Research Center
Motorola Labs, Marlborough, MA

Abstract—Recent large scale disasters have awakened governments domestically and overseas to their needs for preparedness to support homeland security and public safety. First responders of various agencies (e.g., fire department, police, EMS) are often on the front line to assist in managing these events to protect lives and property. The effectiveness of their mission is highly dependent on capability of communication systems available at incident scenes. The US Department of Homeland Security has among its top priorities the need for stronger information sharing and infrastructure protection, as well as interoperable communications and equipments. In this paper, we determine key requirements for first responder systems by examining various vulnerabilities and threats in such systems. We investigate implications of interoperable heterogeneous networking, horizontal/vertical communications and various applications on system architecture design. We also identify technical challenges in designing first responder systems with high quality of service and quality of protection, which are critical for supporting diverse multimedia first responder applications over reliable and trusted heterogeneous networks.

I. INTRODUCTION

Mankind has long been grappling with large scale natural disasters, such as earthquakes, tsunamis, hurricanes, and outbreaks of contagious diseases. Even with accurate disaster prediction technology to order massive evacuation in advance, history has given us insight into the considerable cost to human lives and property when a large scale natural disaster hits without measurable sign of imminence. For example, in hurricane Katrina, which hit the gulf coast of the United States in 2005, at least 1,330 were killed, thousands were injured, and estimated 300, 000 homes were made uninhabitable. Today, mankind faces other kinds of large scale disasters caused in part ironically due to advances in technology itself, and in part increasingly due to (social and economical problems) evil individuals and terrorist organizations, such as terrorism on September 11 of 2001.

Large-scale disasters, both natural and man-made, in recent years have awakened governments regarding the increasing need for improving communication infrastructure to support homeland security and public safety for first responders who keeps us safe and away from harm. The need is diverse. The US Department of Homeland Security exerts among its top priorities on stronger information sharing and infrastructure protection with interoperable communications and equipment [1] [2]. In retrospect, if the cell towers in New Orleans had not been blown over, the communication between New Orleans and nearby large cities/federal departments would not have been dissolved and more timely resource and human aid could have been obtained; if the agencies had been able to talk to each other easily in Sep. 11, 121 firefighters could have been timely informed of the dangerous situation and have survived the tower collapse. We present in this paper diverse requirements and resulting system architecture implications for first responder systems. We hope that the paper will serve as a comprehensive guideline for integrated system design.

First, we will introduce a use case of tunnel collapse to help readers obtain a concrete impression of how first responders work and cooperate together. Then, we will present a broad view of first responder systems briefly from three aspects: network model of the physical communication infrastructure, communication flow at the user layer, and application model. Afterwards, we will focus on the analysis of the incident scene networks because of its unique challenges: (1) it is an ad hoc network with dynamic scale and it is formed even without infrastructure support whenever first responders arrive at the incident scene and dismissed whenever mission is accomplished; (2) seamless communication across incompatible devices and agencies with service differentiation must be supported to protect safety of our officers and people under constrained resource; (3) being deployed in the open wireless space, it is prone to be attacked by terrorists and hackers. Starting from the unique features of the incident scene first responder system and its vulnerability and threat, we propose six design criteria to evaluate the first responder system and five essential management components for a trustworthy and robust communication infrastructure to safeguard against vulnerability and threat and to meet the persistent service requirement.

II. A USE CASE: TUNNEL COLLAPSE

We present a tunnel collapse case to make a concrete image of first responder systems, which is conceived based on the Boston big dig tunnel collapse incident in 2006 [3]. This use case serves as an example to show how incident scene and corresponding management layers get evolved, and how information is exchanged among all the authorized sources and officers.

A. Description

A tunnel of downtown highway collapses during 8:00 AM rush hour. Massive concrete ceiling and steel crashes several...
vehicles. A few other vehicles collide with one another in a chain reaction. More than a dozen people are injured, and a few are trapped in their crushed vehicles. Traffic through this tunnel comes to a complete stop.

B. Participants

1) Law Enforcement:
   Role & Mission: Command and control; rescue trapped victims; investigate crime; traffic redirection; media relations.
   Population: 6 highway patrol officers, 4 public safety officers, a police chief, and 1 FBI agent.
   Communication Requirement: High security, high reliability, and medium bandwidth; mobility at pedestrian speed.

2) Emergency Medical Service EMS:
   Role & Mission: Emergency medical care on scene; transportation to hospitals.
   Population: 5 paramedics, 6 emergency medical technicians, and 1 physician.
   Communication Requirement: Medium security, high reliability, and high bandwidth; mobility up to vehicular speed.

C. Detailed Timeline

8:04 AM: Upon receiving 911 calls, several highway patrol officers are immediately dispatched to the scene to investigate the incident. Recognizing the severity of the incident, one of them calls back to the police headquarters to summon help. Meanwhile they start to search for victims who are trapped in the cars and under the falling cement.

8:07 AM: The police chief arrives at the scene with additional highway patrol officers and a few public safety officers. A mobile command center is deployed at the scene. The police chief checks the tunnel surveillance video to investigate the cause of the incident and monitor the ongoing situation. Meanwhile, some of the highway patrol officers begin to redirect traffic.

8:15 AM: EMS personnel arrive in a second wave and join the first responder system. Several emergency medical technicians begin to perform triage assessment to screen victims. Those who are seriously hurt are immediately transported to nearby hospitals.

8:20 AM: The police use portable PDAs to capture victims’ fingerprints and transmit them to the state/national fingerprint database for identification recognition. Medical personnel begin treating remaining injured victims. Medical records of the victims are remotely retrieved from personal physicians’ databases using electronic identification information from police’s incident log. Recorded via RFID devices mounted on victims’ arms, real-time vital signals are sent to a nearby hospital for remote diagnosis and preparation of the emergency operation on location.

8:35 AM: A FBI agent arrives to investigate and collect intelligence to determine if there is any linkage to terrorism. The public safety officers begin interviewing witnesses and submit electronic reports to a central incident database located in the police headquarters.

10:00 AM: A construction crane is brought in to remove fallen concrete and metal. The police chief conducts a press conference to inform the public about the incident.

III. FIRST RESPONDER SYSTEM FRAMEWORK

First responders, who play critical roles in protection of lives and property, represent personnel from various public safety agencies providing support for law enforcement, EMS, fire control, hazardous material management, public health service, and other mutual aid groups.

A first responder system comprises an incident command system and a wireless communication system [4]. The incident command system manages planning, operations, logistics, administration, and information dissemination, to support first responders deployed in incident scenes under a broad spectrum of emergencies. The wireless communication system is a dynamic mobile multi-hop ad-hoc wireless networks established on demand, with or without existing infrastructure support. Via self-configuring networks formed by devices carried or dropped by responders, and access to backbone networks under the incident command system, first responders exchange information rapidly and securely among themselves, the command center, and remote databases and hence enable cooperative rescue mission and critical decisions.

To avoid confusion by multiple conflicting directives, a chain of command is often formed at the incident scene. The chain encompasses the incident management team of multi-agency staffs. The incident management team resides at the mobile command center near the incident scene. Visually monitoring status and location of all devices and personnel in the scene and surveying lively video, this team coordinates first responders at all magnitudes and allocates resources optimally. Figure 1 shows an example of the first responder system composed of different scale networks (Internet and mobile ad hoc networks) with heterogeneous devices from two agencies: fire fighters and EMS as described in the use case of Section II. Since incident management comprises a wide array of operations to facilitate prevention, preparedness, response, and recovery [5], we will examine the first responder system from three aspects: incident management network model, communication flow among first responders, and public safety application models.

A. Network Models

Hundreds and thousands of devices may be integrated together in order to support the seamless end-to-end user
communication in a first responder system. This complex first responder system can be decomposed into four types of network: PAN, IAN, JAN and EAN according to their scale, function and characteristics [6].

- **Personal Area Network (PAN):** This is a small-scale wireless network used for physical communication among devices (e.g., video camera, RFID) and sensors (e.g., heart rate monitors), carried by or embedded in clothing of a person. PANs are widely used today for health/equipment monitoring and environmental surveillance. The aggregated statistics collected in PAN are first recorded in First Responder’s Communication Devices (FRCD), which then relay event notification back to the command center and other first responders periodically or upon query. The devices are normally plug-and-play devices, supported via secure connection and high data rate over a short transmission range.

- **Incident Area Network (IAN):** This is a multi-hop ad hoc wireless network deployed on demand in the incident area, where communication infrastructures do not exist or have been destroyed. The devices (also referred as nodes) include, but are not limited to, mobile devices (e.g., handheld devices, mobile robotics, and temporary RFIDs) and portable devices (e.g., droppable relay devices, devices mounted on vehicles, and environmental sensors) with vehicles acting as the gateway to outside of IAN.

- **Jurisdiction Area Network (JAN):** This is the private network of agencies, responsible for secrecy database access, certificate management, task dispatch, and resource mobilization via command centers.

- **Extended Area Network (EAN):** This is the backbone network for interconnecting JANs and IANs, as well as provision of public Internet access (e.g., real-time weather from public sites).

In this paper, we will focus on incident scene management in IANs composed of diverse number of PANs. Therefore, we summarize their characteristics in Table 1.

<table>
<thead>
<tr>
<th>TABLE I</th>
<th>SUMMARY OF PAN AND IAN</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Range (m)</strong></td>
<td><strong>PAN</strong></td>
</tr>
<tr>
<td>Mobility</td>
<td>Fixed relative to FRCD</td>
</tr>
<tr>
<td>Scale (devices)</td>
<td>1-10 (1-2 hops)</td>
</tr>
<tr>
<td>Technology</td>
<td>UWB, Bluetooth</td>
</tr>
<tr>
<td>Devices</td>
<td>Camera, heart rate sensor, FRCDs</td>
</tr>
<tr>
<td>Admin. domain</td>
<td>Single</td>
</tr>
</tbody>
</table>

### Relationship and Comparison

In Figure 1, we show the relationship between the four types of networks in the tunnel collapse case. FRCDs link PANs and IANs, and two vehicles connect IANs and JANs for better balanced load. Incident management team resides in one police vehicle. The police and EMS team form two private IAN networks in order to isolate traffic and unnecessary interference; however any desired resource sharing and cooperation among two teams is granted by the incident command center to enable efficient direct communication links among two private IANs.

After authorization, the communication among EMS, police and victims (RFID) is established to share both information and resource (devices and media) securely.

### B. Communication Models

Communication flow within a first responder system refers to a flow of information among first responders in the field and personnel in the incident command system. Triandis [7] suggested, in a generic context, that the user communication flow may be classified in terms of a vertical one where hierarchy is emphasized and a horizontal one where equality is emphasized. We extend this idea to model the complex cross-discipline and cross-jurisdiction communication relationship in a first responder system. This classification guides us to understand information flow, basic requirements and authorization intuitively from the users’ perspectives.

1) **Vertical Communication:** Vertical communication refers to exchange of information among communicating entities at different levels of a command hierarchy in an agency or in a discipline (such as EMS, police). This command hierarchy is similar to a chain of command in an incident command system. The command hierarchy is, from top down, in terms of jurisdictions levels from Federal, State, Regional, to Local authorities inside one discipline, or in terms of individual responsibility from incident commander, task leader, to officers inside one agency. Vertical communication tends to follow a tree-like logical relationship, where the tree of the incident scene is rooted at the command center.

Roles in different hierarchical levels are assigned different priorities and privileges. Role-based access control enables roles near the root to have higher security clearance and authority than those near the leaves. For example, in the tunnel collapse case, incident commander is authorized to query location and status information of any police officer, while a police officer is only authorized to query his own location and status information. In addition, policy-based service differentiation, such as preemption, is provided when two first responders at different hierarchy levels contend for shared resources, such as wireless channels.

2) **Horizontal Communication:** Horizontal communication refers to the exchange of information among first responders belonging to the same or different agencies. Communicating peers are in the same administrative level. Horizontal communication tends to follow a mesh-like logical relationship, where the relationship is denser among entities within an organization and less dense across different organizations.

Service differentiation in horizontal communications depends mainly on content and purpose of each communication session. For example, EMS personnel may preempt investigator and voice communication is preferred over bulk file transfer.

We notice that communication usually happens in a group of entities across and within administrative domains. Users are grouped dynamically based on missions for the reason of easy management. Information is seamlessly shared inside a group while is isolated among groups to avoid leakage of sensitive data. The vertical and horizontal communications are usually called a peer-to-peer communication; whereas, group-based communication is a composite of vertical and/or
horizontal communication, where multiple peers are connected in a multicast way.

C. Application Models

To support informed day-to-day routine and emergency response, diverse multimedia applications (e.g. text, audio, graphics, video and interactive command) are present in the first responder system. The information includes three types of content: voice, data and video. Generally this information is independent of the underlying network devices and protocols.

1) Voice: relays command, instruction and advices in a peer-to-peer or multicast mode timely. It is the most common data format with strict timeliness requirements;

2) Data: of texts and graphics inform first responders about the situation. The data come from authorized databases, such as the state motor vehicles database, and building information; and commands are delivered to and reconfigures devices. One example is the electronic crime report submitted for permanent logging;

3) Video: bolsters surveillance and audit by recording the entire history and enables remote meeting and assistance. With the advance of wireless and p2p technology, online video communication and offline storage with high bandwidth, low delay and jitter is not impossible. A case in point is the surveillance video in the scenario of tunnel collapse.

IV. VULNERABILITIES AND THREATS

The first responder system represents a complex system, which leads to unavoidable vulnerability and security threats.

A. Vulnerabilities

First responder systems are susceptible to performance degradation and failure, due to a variety of environmental, system, and operational factors as follows.

Environmental Factors: First responder systems typically operate in a very harsh propagation environment through wireless channels. The communication is likely affected by channel fading, multi-path fading, and interference from background noise and neighbors, which makes the reception of the packets probabilistic and hard to decode. Increased number of retransmissions induces high end-to-end delay and delay variance, and degrades effective bandwidth using inferior transient routes

System Factors: System factors come from non-uniform user density and connectivity, as well as component failure/malfunction and frequent user movement. Due to the task-centric mobility pattern, non-uniform network topology brings negative impacts on coverage and load balance. Even though widely used droppable radio bridges improve network connectivity and divert traffic away from hot-spots, it is still unclear when and where to deploy them in a cost-effective way and the appropriate number. Component failure and malfunction caused by hardware or software faults represents another type of vulnerability. Commonly operating in electronically-unfriendly environments, such as a building on fire or a flooded village, first responder systems are prone to hardware failures. Software failures are unavoidable in complex systems with bugs and protocol incompatibility as well. Systems factors make the network topology and scale unpredictable and therefore, it is important to ensure reliable and persistent connectivity even with unstable link quality and transient routes and to ensure fast self-recovery with minimal human intervention.

Operational Factors: Operational issues arise when heterogeneous devices, protocols, networks and applications merge in a cooperation-demanding environment composed of multiple agencies of different administrative domains and policies. Issues of incompatibility are akin to be raised with legacy devices, proliferation of networking protocols (standards as well as proprietary), network prototype (e.g. sensor, ad hoc, cellular networks) and outdated security technology. In addition, the computational power and functionality of devices are unequal. Upon resource sharing and information exchange, many agencies often do not communicate well due to technical and policy barriers;

B. Threats

Ease of deployment and mobility of wireless ad hoc networks has promoted their fast development and widespread use; however, these networks have become hotbeds of crime and hacker's gadget as well, due to broadcast and open access characteristics. Therefore, first responder systems are prone to malicious attacks by unauthorized outsiders/users and intentional abuse by malicious/misbehaving insiders. We group threats into three types:

(a) Denial of Service (DoS)

Attackers could deny granted services to legitimate users. There are three known genres of DoS attacks:

1) Flooding a network: Easy breach of the unenforced wireless Media Access Control (MAC) protocol allows attackers to rob an unfair portion of bandwidth. In network layer, attackers could inject large volume of false packets to congest the networks. Worst of all, jamming the physical channel totally disables communication;

2) Disrupting connections between peers: Attackers could either confuse routing protocols by spoofing, altering, or replaying routing information so that data packets fail to arrive at the destination. Attackers may selectively drop, delay, reroute and delay data packets at different time or locations to adversely affect reliability and performance of the transport protocol;

3) Preventing a particular user from accessing services: Attackers could defame other legitimate users by propagating forged blacklists.

(b) Data Manipulation

Besides communication mechanism, messages being transmitted are under threat as well, whose contents represent user data, trust and activity information.

1) User data: Attackers could eavesdrop and modify packet content; they can replay, reroute and delay packets as well;

2) Trust information: This information is used to establish the critical and trustworthy communication across stacked layers, and it is the target of attacks. Authentication key could have been stolen or fabricated to grant illegal access with no duplication detection and synchronized revocation mechanisms. Faked devices can defame other well-behaved devices by sending false
blacklists and trigger system entering costly alarmed states;

3) *Activity information:* Simply monitoring the volume of all incoming and outgoing traffic can give away activity information, for example, a launch of a mission.

(c) Physical Attacks

Attackers could simply destroy the devices physically. If the functionality of devices is not duplicated sufficiently or the critical devices are not under close protection, destroying several of them could impair those important functions, for instance, protocol proxy between two technically incompatible administrative domains.

Worst of all, collusive attacks are difficult to detect and have notorious impact. Even a small number of colluders may demolish a significant portion of communications.

V. SYSTEM REQUIREMENTS, DESIGN CONSIDERATION AND THEIR ARCHITECTURAL IMPLICATIONS

In this section, we present our broad view of an integral architecture with essential components to support a robust and efficient incident scene communication network [8]. We also identify six design criteria needing to be incorporated into first responder systems and their relative value associated with different components.

A. Architectural Implications

We show the following indispensable architecture components in Figure 2.

1) Environmental surveillance management: Surveillance sensors and cameras dramatically boost the effectiveness of officers’ mission and their controlling capability. They support navigation to guide users and robots towards targets through a safe and short path [9]; they aggregate the status of surrounding devices and alert users when to replace the malfunctioning devices and what set of devices are detected to be misbehaving, hence leading to security threat; they monitor officers’ health so that timely treatment can be given upon emergency.

To make surveillance and monitoring a practice, many questions need to be answered, such as the in-network aggregation, compression of status and event description, authentication and authorization of personal statistics access (privacy-preserving data management) and cross-organization co-sensing network.

2) Topology management: Ad hoc network with dynamic scale as well as the plausible vulnerability from environmental and system factors make the network connectivity unstable and therefore degrade the end-to-end service performance. As a result, topology management needs to be there to hide those vulnerable and unstable factors.

The common methods to control topology are combined power control (k-connectivity networks) and routing, and exploitation of the orthogonal channel, path and user diversity (mobility). Different from avoidance, early detection and preparation are alternative ways to elevate system-level robustness against vulnerability. When the connection is perceived to shamble, extra droppable radio bridges are deployed at strategic places. Careful design of hardware and software is also helpful to avoid system failure, such as environmental hardened components, hardware redundancy, and remote software updates to fix the troublesome bugs online.

3) Mobility management: In a common incident area, devices move at different speeds. Realistic mobility pattern, such as a group-based task-centric geographically-constrained moving pattern should be assumed for IAN, rather than random-way point mobility pattern assumed mostly in current mobile network simulation. Mobility management is used to support seamless physical movement as wished by welcoming asset and avoiding liability (such as uneven device density). By tracking where the sender, forwards and destination are and predicting their movement, efficient handoff processes can be implemented early before the perceived link quality drops and avoids route discovery delay, especially when roaming across agencies. Furthermore, mobility management improves both network capacity (via carry-store-move-forward network prototype) and security (via direct secure association without intermediates).

Another aspect of mobility management is to provide basic location services to pinpoint any mobile device. One direct application of such service is geographic routing to avoid bandwidth consumption of network-wide flooding during the route discovery.

4) Trust management: Conventional trust management is in the form of membership management where trust is represented as a binary value. Through role-based access control, the access to various services and data resource is authorized to the person with the right privilege after successful authentication. However, this simple access control model is not valid in first responder systems due to the existence of threats and multiple administrative domains. Trustworthiness of devices can change frequently due to operating environment, compromise by attackers and cooperative relationship among agencies. Therefore a static membership system should be replaced by a distributed trust management system. Questions in trust management are: a) how to codify, analyze and manage a trust decision in a distributed and light-weighted fashion, b) how to quantify trust and how much trust to allocate to someone to take an action on particular objects (on someone’s behalf) and c) how to utilize trust.

Broadcast-based wireless media enables us to detect the inoperative, greedy and compromised nodes via monitoring and election. Trust adjustment is based not only on misbehavior but also on the context: a good node near attack is assigned a low trust value due to the likelihood being attacked. By assigning different weights to nodes and their message, a self-driven trust management could be implemented on top of detection and trust gossip. The key components include...
trust calculation module, alert/recommendation import module (reception, filtering and evaluation), and alert/recommendation export module (filtering and selective-transmission).

Some intuitions to evaluate and allocate initial trust are: assign more trust to those high in the hierarchy of the vertical communication, inside the same administration domain and with advanced technology to resist compromising.

One advantage of trust is its ability to defeat the defaming and slander attacks with extended idea from quorum and voting. The trust systems can also interact with applications, routing software and quality of service components to prevent threats by avoiding, containing, resisting and isolating less trustworthy nodes. Intelligent routing protocols bypass low-security zones when transmitting sensitive data; upon detecting unfriendliness, nodes switch to defensive and costly mode and the less trustful nodes are discriminated.

To make the trust management system feasible, authentication is a critical step for identity binding. Compromise-resilient and efficient key management scheme prevent sybil attacks [10] and furthermore, tamper-resistant hardware platforms reduce the possibility of leaking stored secret key out even if the devices are physically captured by attackers.

5) Data Management: A variety of quality requirements must be fulfilled under capability constraint of devices, such as memory, computational capabilities and transmission power. Quality of Service (QoS) for high priority flows pays the price of reduced utilization of network resource; quality of protection (QoP) requires additional trust maintenance component with increased communication and computational overhead. Thus we must balance between QoS, QoP and resource utilization in an integrated utility function. The integrated design principle also comes from the observation that QoS and QoP are tightly coupled with each other. Without support of QoS, key materials can be delayed due to congestion or loss of control data, thus leaving security holes in the trust management. Without QoP, QoS mechanism is prone to be attacked, such as flooding faked high priority packets, flooding QoS control messages and flow analysis.

Other components we envision are statistical survivability analysis, placement of performance and security functions and intermittent hibernation and wake-up scheme.

B. Design Criteria

Based on the discussion above, we summarize the essential features for the requirements of first responder systems, in terms of the following design criteria and their relative value to each component.

1) Interoperability: It is necessary to improve the ability to exchange information across organizational domains with different security policies and service level agreements;

2) Scalability: It is necessary to accommodate different scales of users and devices throughout their phased deployment and withdrawal;

3) Service differentiation: It is necessary to provide different priorities to users or flows according to vertical communication hierarchy, and soft-guarantee performance to real time applications, such as interactive voice conversation;

4) Adaptiveness: It is necessary for the whole first responder system to be self-organizing, self-recovering and adaptive to the incident context without human invention or minimal;

5) Robustness: It is necessary to provision robustness against potential system failures, quality of service against offered load surge, and correct operation even in severe environmental conditions;

6) Security: It is necessary to improve the trustworthiness and privacy of information exchange, such as encryption, authentication, authorization and redundancy against eavesdropping, impersonating, and denial of service.

TABLE II
ARCHITECTURE COMPONENTS AND DESIGN CRITERIA

<table>
<thead>
<tr>
<th>Architecture Components</th>
<th>Design Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Environmental surveillance</td>
<td>Interoperability, Scalability, Adaptiveness, Robustness, Security</td>
</tr>
<tr>
<td>Topology</td>
<td>Scalability, Adaptiveness</td>
</tr>
<tr>
<td>Mobility</td>
<td>Robustness, Adaptiveness, Security</td>
</tr>
<tr>
<td>Trust</td>
<td>Scalability, Robustness, Security</td>
</tr>
<tr>
<td>Data</td>
<td>Interoperability, Service differentiation, Security</td>
</tr>
</tbody>
</table>

VI. CONCLUSION

We have studied the fundamental requirements and challenges of first responder systems from various perspectives. The ultimate vision is to build an interoperable mobile and trusted network on the incident scene in real time, to maximize the resource sharing and network utilization and to support different types of mission-critical services. Furthermore, to minimize impact of various vulnerabilities and protect the first responder system from various threats, the system must be designed to adapt to dynamic environmental factors and to be robust against malicious attacks.

REFERENCES


