ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
Published By: **Oriental Scientific Publishing Co., India.**
www.computerscijournal.org

ISSN: 0974-6471
March 2013,
Vol. 6, No. (1):
Pgs. 01-16

A Paper in Mobile Ad-hoc Networks about Maintaining its Survivability

SOHAIB AHMAD, FAHEEM KHAN, MUKHTAR AHMAD , SHAZIA NAEEM, M.N .KHALID and ASIA BEGUM

Islamia College University Peshawar, KPK Pakistan
Gandahara University Peshawar, KPK Pakistan

(Received: January 10, 2013; Accepted: January 25, 2013)

ABSTRACT

In general, Security techniques pursue two defense lines: one preventive and the second one is reactive[6]. The first one offers techniques to circumvent any type of Attack, as firewalls and cryptographic systems. The second consists in getting act on demand to lessen Intrusions, as Intrusion Detection systems. This paper observes Survivable approaches whose purpose is to facilitate network s to complete their functions properly and significantly even In the presence of Intrusions. preventive, reactive techniques and Tolerance defense lines. This paper established Survivability concepts and its association with preventive, reactive and Tolerance defense lines. Survivable MANETs will be capable to accomplish their purposes and aims by means of the cooperation between those three defense lines. Key Properties of Survivability as resistance, acknowledgment, recovery and adaptability were thorough, and Survivability needs for MANETs were examined. In conclusion, this function highlights that a completely Survivable MANET be supposed to be appropriate cooperatively the three defense lines as an alternative of only one or two lines separately.

Key words: Survivability, Intrusion Tolerance, MANETs, Security.

INTRODUCTION

The word MANET (Mobile Ad-hoc Network) refers to a multi-hop Packet Based Wireless network composed of a set of Mobile Nodes that can exchange Information and at the same time move, without using any kind of permanent infrastructure. MANET is In fact self Organizing and Adaptive network s that can be formed and deformed on the fly without the requirement of any Centralized administration. As for other Packet Data network s, one to-one Communication Ina MANET is attained by unicast Routing every single Packet. Routing In MANET is exigent due to the limitation presented on the transmission Bandwidth battery power and CPU time and the need to manage with the repeated topological alterations resultant from the mobility

of the Nodes.

Nodes of a MANET cooperate In the job of Routing Packets to Destination Nodes, as each node of the network is capable to exchange Information only with those Nodes located inside its transmission radius R, while the source and Destination Nodes can be located a area very higher As the significance of computers In our everyday life enhances it also situates new difficulty for connectivity[1]. Wired infrastructure solutions have been around for a long time but there is increasing claim on functioning Wireless solutions for linking to the Internet. There are solutions to these requirements, one being Wireless local area network that is based on IEEE802.11 standard. On the other hand, there is increasing requirement for connectivity In situations where there is no base station (i.e. backbone connection) available (such as two or more PDAs requirement to be associated). This is where ad-hoc network s step in[2].

MANETs are regularly defined as pursue: A "Mobile ad-hoc network" (MANET) is an independent System of Mobile routers linked by Wireless links the combination of which figures an arbitrary graph. The routers are free to move randomly and organize them arbitrarily; thus, the network's Wireless topology may vary fast and randomly. Such a network may function Ina standalone style, or may be linked to the bigger Internet. The potency of the link can vary quickly In time or even vanish totally. Nodes can emerge, vanish and re-emerge as the time goes on and all the time the network links should function among the Nodes that are part of it[3]. Ad-hoc network s are network s are not linked to any wired infrastructure. An ad-hoc network is a LAN or other small network, particularly one with Wireless links, In which some of the network devices are part of the network only for the period of a Communications session or, In the case of Mobile devices. The ad-hoc network is a Communication network without a pre-exist network infrastructure. In cellular network s, there is a network infrastructure symbolized by the base-stations, Radio network controllers, etc. In ad-hoc network s every Communication terminal (or radio terminal RT) exchange Information's with its collaborator to execute peer-to-peer Communication. If the important RT is not a neighbor to the commence call RT (exterior the exposure region of the RT), then the other intermediary RTs are used to execute the Communication link. This is described as multi-hope peer-to-peer Communication. This association among the RTs is very significant In the ad-hoc Networks. In ad-hoc Networks all the Communication network Protocols should be Distributed all through the Communication Terminals (i.e. the Communication Terminals should be autonomous and extremely supportive) because of explanation limitations and MANETs distinctiveness, Researchers have paying attention on scheming Security techniques for getting network Survivability[4]. Survivability is usually described as the capability of a System to accomplish its task, Ina appropriate approach, In the occurrence of Attacks, failure or disaster[5]. The term System has an extensive meaning and could distinguish network s, way of Communication or services, and operation corresponds to the conceptual purposes and requirements of the System.

The paper is organized as follow

(i) To consider a planned viewpoint about resiliency-oriented method with the conceptualizations of Survivability to Attacks.

(ii) Signifying that Survivability to Attacks can be achieved when all defense lines function are helpful to each other.

(iii) The recognition of Survivability requirements and Key Properties for MANETs;

(iv) The examining of Survivable Initiatives, which are arranged In three groups: route discovery, Data transmission and key management

The remaining of the paper is organized as follows.

- Section II defines Survivable systems, present Survivability concepts and Key Properties, In addition to an organization of defense lines allowing for those ideas.
- Section III summarizes Manet's characteristics, Security issues and usual countermeasures.
- Section IV examines the Survivability

requirements for MANETs, getting into account their necessary services.

- Section V explains and classifies in three groups the Survivable Initiatives for MANETs.
- Section VI Explain its Technical Background.
- Finally, Section VII explains and wrap up the paper and presents Future guidelines

Key properties and concepts about survivability

In general, Security techniques pursue two defense lines: one preventive and the second one is reactive[6]. The first one offers techniques to circumvent any type of Attack, as firewalls and cryptographic systems. The second consists In getting act on demand to lessen Intrusions, as Intrusion Detection systems. On the other hand, preventive and reactive methods are not proficient to put all Attacks and Intrusions off[7-8]. Thus, Research groups have brought together Security techniques In the direction of one-third-defense line, called Intrusion Tolerance (IT)[8], as shown In figure 1.

Survivability directed towards a System potential of carrying out its purposes and needs Ina well-timed approach In face of Attacks, Intrusions, failure or calamity[9]. Laprie *et. al,*[10] believes Survivability analogous to reliability In provisions of purposes and addressed coercion. Dependability purposes consist In the System capability of distributing dependence services and circumventing the very recurrent or stern malfunctions. This function addresses Survivability as a particular case of dependability, where the network is capable to fulfill its purposes In the presence of malevolent mistakes. These errors show diverse circumstances and particular requirements that can simply be proficiently treated when examined independently. Hence, Survivability endeavors to enhance Security success, and aid dependability and Security integration. Survivability features are reliability, availability, main- attainability, confidentiality, integrity and security[10].Survivable systems address a subset of errors, called malevolent or calculated errors, containing of malevolent logics and DoS Attacks or Intrusion. Generally, these errors mistreatment of existing System vulnerabilities, established by accident or on purpose throughout the development of the System. An Attack can effectively utilize System vulnerabilities resultant In an Intrusion. This function proposes that Survivability be supposed to be achieved by the use of preventive, reactive and tolerant approaches working mutually.

Resistance is the capability of a System to keep away Attacks. User verification, firewalls and cryptography are examples of techniques used to accomplish it. Recognition is the System capability to identify Attacks and assess the degree of harm. Examples of recognition techniques are Intrusion Detection by outlines and internal System integrity confirmation. Recovery is the potential of renovating disturbed Information or functionality inside time restraint, restraining the harm and maintains necessary services. Traditional strategy functional for attaining recovery is duplication and redundancy. In conclusion, adaptability is the System capability of rapidly incorporate lessons learned from failures and adjusting to rising intimidation[9]. Examples of adaptation procedures are the topology Control by the radio power management and active networking technology. The application of active networking technology proposes to permit the dynamic selection of MAC or network layer parameters, and the dynamic compromise of algorithms and whole Protocols Based on application needs or the Communication environment. Figure3 shows the interaction among these Key Properties.

Techniques and related problems issues and for security inmobile ad-hoc network

Mobile Ad-hoc Networks are vulnerable to many Security issues. Characteristics as dynamic topology, resource restraint, restricted physical Security and no centralized infrastructure make those network s susceptible to passive and active Attacks. In passive Attacks, Packets having secret Information may be snooped, abusing the confidentiality standard.

Active Attacks contain inserting Packets to illogical Destinations, erasing Packets, transforming the substance of Packets, and impersonate other Nodes.

The classification of Attacks by network

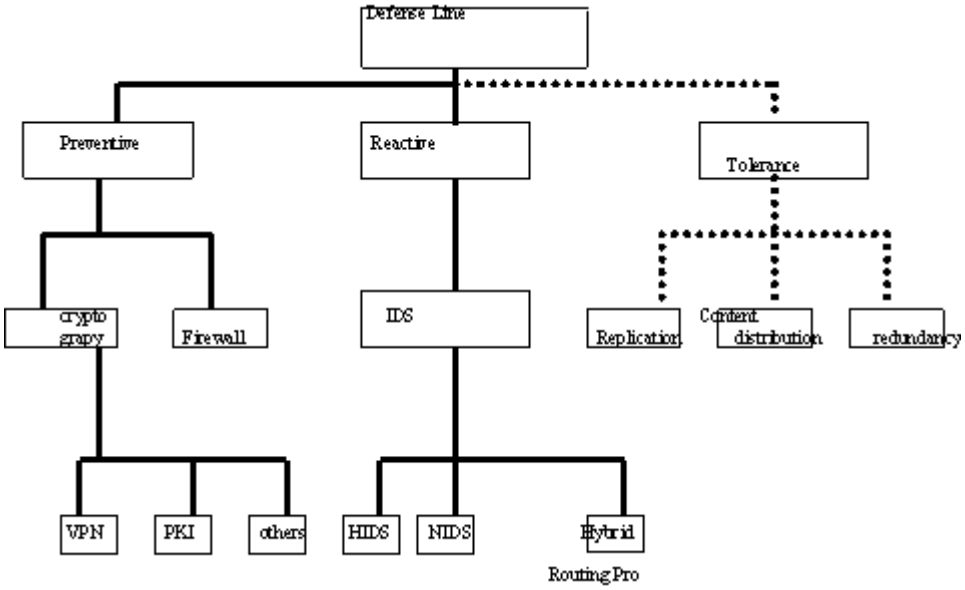

Fig. 1: New classification line of defense

Protocol stack is the further recurrent. Table I sum up the major Attacks for MANETs according to network layer Some Attacks are also grouped as Byzantine or misbehavior Attacks, being produced by network.

Node whose measures cannot be dependence or do not be conventional to Protocol Specifications. Black hole, worm- hole, Rushing, Sybil, sinkhole, HELLO flooding and Selective forwarding are examples of Byzantine Attacks. In addition, these Attacks are also connected to selfishness issue. The purpose of a selfish node is to make use of the benefit of contributing In the ad-hoc Network without having to disburse its own resources In exchange. Researchers have actively discovered many techniques for protecting Mobile ad-hoc Networks. These techniques are based basically on customized cryptographic primitives, Protocols for path diversity, Protocols that eavesdrop on neighbor communication, and Protocols that use particular hardware[11].

Cryptographic primitives have been used to offer Authentication, integrity and confidentiality of safe Routing Protocols[12-14]. Generally, HMAC (message Authentication code used for verification[28]), digital signatures and symmetric or asymmetric cryptographic operations are functional with these reasons. On the other hand, this mechanism usually enhances the network overhead. MANET restraint resources avoid the practice of composite encryption techniques. In addition, no presence of infrastructure and dynamic topology enhance the complexity for the Key management and distribution, and mostly these techniques cannot protect In opposition to internal Attacks. Path diversity procedures plan to enhance route Robustness by discovering Multi-path routes and by these paths to offer redundancy In Data transmission[11,15,16]. Multi-path Routing Protocols can use all routes found at the same time and send out the same Data more than one time; or can use them on demand, as an option. On the other hand, many of those Protocols do not relate techniques to validate intermediary Nodes In routes, make them susceptible to impersonation and Sybil Attacks Procedures for observing neighbor Communication and performance In Wireless channel have been planned to identify and reduce misbehaving Nodes[11,17]. Usually, these procedures suppose that Wireless interfaces maintain promiscuous mode operation. Promiscuous mode means that if a node Ais inside range of a node B, it can eaves drop

Communications to and from B even if those Communications do not openly engage the node A. By means of this technique, Nodes can observe others and broadcast those that have misbehavior as falling or tamper Packets. In conclusion, hardware, as GPS (global position System) or directional antennas, has been used to help In stopping and identifying wormhole Attacks. Pering et. al, such as, initiate the idea of Packet leash as a general mechanism for identifying and defending beside them . A leash is any Information added to a Packet and calculated to limit its transmission space. Leashes are classified as Geo graphical or temporal. A Geo graphical leash guarantees that the recipient of the Packet is inside a definite space from the correspondent, and to get localization locations, the GPS can be used. In[18], a directional antenna method was planned to also identify those Attacks. The method limits the Communication between Nodes Based on distance Information, which is intended according to got signals. Unluckily, these methods are precise to wormhole Attacks.

For manets sustainability; survivability requirements

Mobile Ad-hoc Networks commence various functions, operations and services inclined by the context, applications and basic characteristics. In important circumstances, where parts of a System are negotiation by Attacks or Intrusions, precedence is given to preserve correct functionality of necessary services. Necessary services demand capacities and assurances to ensure their accurate deliverance Inthe presence o attacks, failure or accidents.

Such capacities and assurances are recognized as Survivability needs and they can deviate considerably depending on the System characteristics, its extent, and the result of the service intermission. In spite of Linger *et. al.,*[19] describe those needs In terms of necessary and unneeded services, this Section confers Survivability needs for MANETs allowing for necessary services and network characteristics. Necessary services In MANETs can be classified In two types: Specific services and general services. The previous signifies those services intended by application or network context. The later denote basic services that are autonomous of applications or context as routing, connectivity and Communication. As Specific services can differ with application or context, this function examines the Survivability needs related to general services. Survivable MANET's have to preserve a linked network even In unfavorable conditions, as that service permits proficient Routing and End-to-End Communication. As a result, Survivable network s must (i) Consider node Heterogeneity balancing their operations and responsibilities amongst the network Nodes; (ii) be capable to vary dynamically the parameters of the links such as Node's addressing and service discovery (iii) be capable to regulate send out powers of Nodes Adaptively In reply to mobility, action needs such as QoS level, environmental circumstances and Attacks and (iv) use Node's energy and other resources efficiently when the System infers that it is under Attack (Efficiency). Routing is another important service whose cooperative way of function carries many Security limitations. Hence, Survivable network s requirement to affect techniques to (i) Control the access of Nodes In the network (access Control); (ii) defend the Wireless Communication at physical and Data link layers with user/Data acquisition (protection); (iii) ensure integrity, confidentiality and verification principles; (iv) present robust and efficient routing; and (v) tolerate Attacks by means of Intrusion Tolerance procedures such as unnecessary approaches Multi-path, two times Routing Protocol and others (redundancy). Communication is the major reason of any network, and Security or mobility issues make MANET's Communications challenge. In this fashion, its Survivability needs consist of (i) designing Protocols that function In general on dissimilar and difficult circumstances (self-adaptation); (ii) making functional End-to-End Communication without need a consistent return channel for acknowledgments; (iii) using multiple Communication channels (redundancy); (iv) arranged through ultimate disengagement and along with incomplete segment of paths (Robustness). Table II summarizes MANETs Survivability these needs getting into account the general services. Definite Survivability needs is outcome of network characteristics. Survivable systems for MANETs cannot have the central point of failures/Attacks. They have to be completely

decentralized and they have to attain the essential organizational arrangements without needing human interference (Self-Organization).Survivable MANETs have to be scalable to think the enormous inconsistency on the total number of Nodes and the dynamic topology. They should also be self -managed and self -Controlled, that is, autonomic to warranty network functionality and Efficiency. Survivable MANETs have to be self -diagnosed observing themselves and finding defective, unavailable, misbehavior or malevolent Nodes. They have to avoid interruptions or improve from issues that may have occurred and find an alternative means of using resources and reconfiguring the entity to be In regular operation (self-healing).Survivable network s have to finally manage themselves In order to optimize the use of their resources, reducing latency and preserving the feature of service. Figure4 shows the integration between all stated needs, prominence those yielded by general important services (light gray) from those shaped by network characteristics (dark gray). The needs reliant of the context or application are not measured; make this imperfect vision In the figure. Each need, as shown InFigure4, is linked to others that jointly can get better the network Survivability. Robustness, such as, will be more efficient for Survivability when redundancy, access Control and safety are also practical. Protection is frequently reached by verification, integrity and confidentiality. Access Control concerns usually verification techniques and self -Controlling characteristic increases it. Scalability need will be reached by means of self -management, self -Organization and self -Controlling. These integrations only show some potential for jointly refining the Survivability, without putting out all of them. Nowadays, each important service In Table II, connectivity, Routing and Communication, is treated and linked to three dissimilar layers, correspondingly, link, and network and application layers. This is not adequate for getting a complete Survivable System due to multi-Layer Attacks. More, the use of multi-Layer Information can make Security techniques more robust, opposed to and Survivable. Routing layer, such as, can use energy or Bandwidth Information there In link layer to get improved options and to be more Adaptive. Routing layer can inform the others about Attack Detection and In this means; those layers can begin an attentive process. In summing up, the Survivability present on the layers can equally offer security and sustainability. Based on these earlier concerns and on the Survivability Key Survivability properties presented In Section II, we acknowledged three

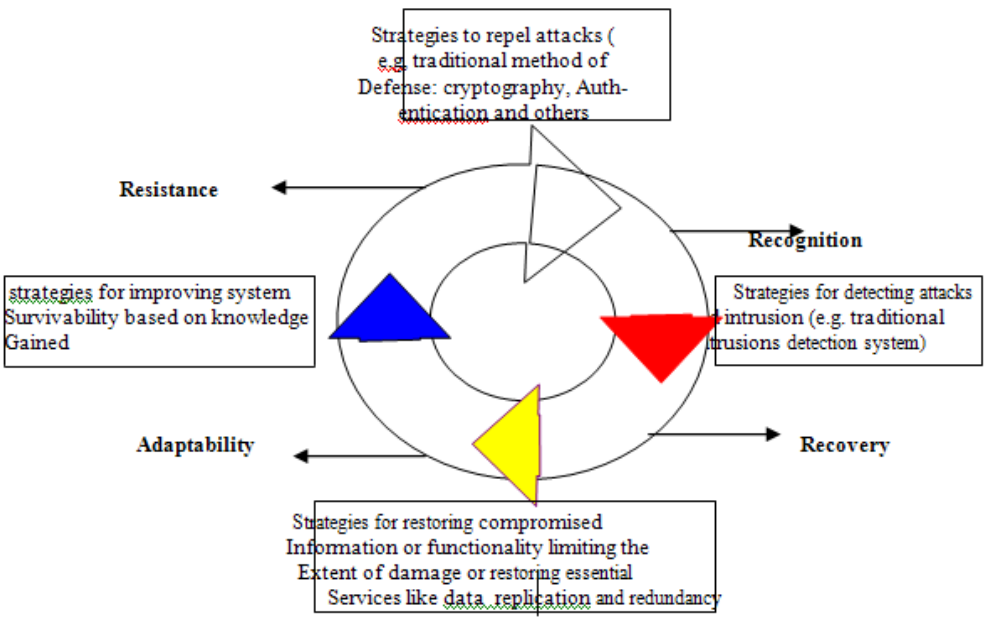

Fig. Survivability key properties

Table 1: Attacks network layer

Layers	Attacks	Description
Physical	Jamming	Deliberate Interference with radio reception to deny the target use of a Communication channel.
Link	Exhaustion	Attacker induces repeated retransmission attempts In order to Exhaust target resources.
	Collision	Deliberate Collision or corruption induced by an Attacker In order to deny the use of a link.
Network	Wormhole	Adversaries cooperate to offer a low- latency side channel for Communication by means of a second radio with higher power and long-range link.
	Black hole	Malevolent nodes manipulates Routing Packets In order to contribute of Routes and then drop Data Packets
	Sinkhole	An try is made to attract traffic from the network to exceed throughout anAdversary In order to assist other Attacks
	Flooding	Overwhelm victims restricted resources: memory and Bandwidth
	Selective forward	Malevolent nodes act as a normal node but they drop sensitive Packets of application
	Sybil	Multiple fake identities will create problems for Adversary nodes.
	Rushing	This attack can carry against on demand routing protocols.
Transport	SYN Flooding	Adversary send many connection request to a target node Overwhelm its resources

view planes for Survivable systems, as shown InFigure5. In the first one (Key Properties), we have the Properties that must be achieved by the System. In the second one (needs), we highlight the needs that Survivable systems requirement to reach. Finally, In the third one (Protocol layers), we highlight that all network layers requirement to be addressed by the System. We note that a whole Survivable System focus these three planes.

Manets initiatives for survivablity

This Section explains a number of Initiatives on structure Survivable Mobile ad-hoc Networks. In spite of that a lot of them do not present a total Survivable suggestion, they have purposes, characteristics and techniques more connected to Properties and needs of Survivability than just preventive or reactive methods. this function focuses on Security proposition that combined more than one defense line and affect some procedure of Tolerance as redundancy or improvement. Initiatives found In the literature are classified on three main groups: route discovery, Data forwarding, and Key management and access Control. The route discovery group consists of approaches demanding to make route discovery phase of Routing Protocols additional resistant and tolerant to dissimilar kinds of Attacks and Intrusion. The Data forwarding group is composed of Initiatives particular on Data forwarding using preventive or reactive Security methods and some Tolerance procedures, as redundancy. The last one contains cryptographic Key management and access Control approaches build to be further tolerant to Attacks Solutions. The majority of the presented Protocols have supposed MANETs as a confidence environment. On the other hand, as shown In earlier sections, MANETs are extremely susceptible to Attacks due to their characteristics. safe Routing Protocols have been projected such as SRP[15], SAODV[20], SAR[21]. These protected Protocols are typically based on verification.

Route discovery

Routing is important for the accurate operation of MANETs, and numerous Routing Protocols have been planned In the literature, counting proactive (table-driven), reactive

(demand- driven), and hybrid Attacks off. In this way, some Research groups have manufactured Intrusion tolerant Routing approaches, such as TIARA (procedures for Intrusion-resistant Ad-hoc Routing Algorithms)[22], BETR (Best-Effort Fault Tolerant Routing)[23], ODSBR (An On- Demand Byzantine Routing Protocol)[24] and BA (Boudriga's Approach)[25].

TIARA

TIARA describes a set of design procedures to lessen the blow of Denial of Service (DoS) Attacks and can be functional on Routing Protocols to permit the satisfactory network operation In the presence of these Attacks. The major procedures recognized by TIARA are: flow-Based route access Control (FLAC), Distributed Wireless firewall, Multi-path routing, flow monitoring, source-initiated flow routing, fast verification, the use of sequence numbers and referral-Based resource allocation.For its effective implementation. In the FLAC procedure, Distributed Wireless firewall and a limited resource allocation are applied together to Control Packet flows and to prevent Attacks Based on resource over- load. Each node participating In the ad-hoc Network contains an access Control list, where authorized flows are defined. A threshold is defined for allocating limited amount of network resources for a given flow. Many routes are discovered and maintained, but only one route is chosen to Data forwarding.

The flow monitoring procedure verifies the network failures transferring periodic Control communication, called flow status Packets. If a path failure is recognized, a substitute path found In the discovery phase will be chosen. The verification procedure In TIARA consists In insertion the path label of the Packet Ina secret location. Every node can classify a dissimilar location for the label inside the Packet being its verification Information.

BETR

Best-Effort fault-tolerant Routing (BETR) is a source routing algorithm discovering path redundancies of ad-hoc Networks. Its purpose is to preserve Packet Routing service with high escape ratio and low overhead In the presence of misbehaving Nodes. BETR by no means efforts to end whether the path, or any node along it, is superior or dreadful. It takes into account presented Information to decide the very practicable path, such as each one with the maximum Packet deliverance percentage Inthe instant past. By means of presented Information and recipient opinion, diverse types of Attacks can be unclearly identified such as Packet dropping, corruption, or misrouting. BETR is based on DSR flooding to recover a set of paths between source and Destination Nodes, when essential, and it selected at first the shortest path to mail Packets. If a route failure is statement, the Protocol will throw away the present Routing path and carry on with the subsequently shortest path In the route cache. The

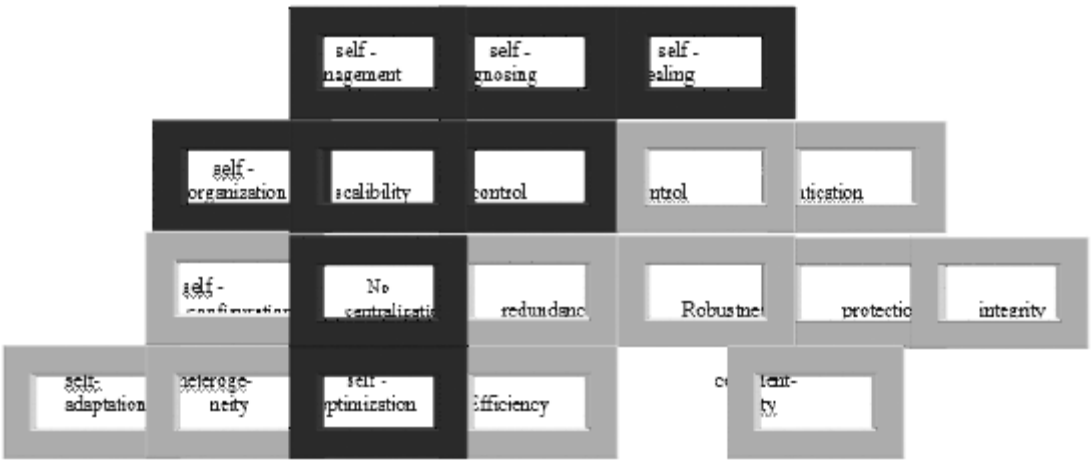

Fig. 4: Integration among survivability requirements

algorithm believes that the performance of any high-quality node is to release Packets properly with elevated deliverance proportion. This way, a good path consists of Nodes with lofty delivery proportion. Any path with small delivery ratio is thus redundant and reinstated by the subsequently shortest path. BETR needs no Security maintains from intermediary Nodes. The source and Destination Nodes of links are supposed well mannered. A earlier dependence association among end Nodes is essential, being probable the verification among them through Data Communication.

Table 2: Survivability Requirements

Essential Services	Survivable System Requirements
Connectivity	Working on heterogeneous network s self -configuration Self -adaptation of node transmit powers In response to mobility, activities, environments and attacks The efficient use of nodes energy
Routing	Node access control Protection of Wireless Communication at physical, medium and data link layer Integrity, authenticity and confidentiality principles Efficiency and Robustness Use of redundant approach
Communication	Working Indifferent and variable conditions Use of asymmetric and unidirectional link End-to-End communication without using reliable return channel Use of multiple communication channel Working even In eventual disconnections

ODSBR

ODSBR is a Routing Protocol that aims to offer a accurate Routing service even In the presence of Byzantine Attacks[26]. ODSBR manages using three sequential phases: (i) slightest weight route discovery, (ii) Byzantine fault localization and (iii) link weight management the first phase is based on double secure flooding and plans to discover lowly cost paths. Double flooding means that route discovery Protocol floods with route request and response messages In order to make sure path setting up. In this phase, cryptography operations ensure secure verification and digital signature. The second phase finds out faulty links on the paths by means of an Adaptive probing procedure. This procedure uses periodic secure acknowledgments from intermediary Nodes along the route and the integrity of the Packets is guaranteed by cryptography. The last phase of ODSBR Protocol manages the weight allocated to a faulty link. Each faulty link has a weight to show dire links, being this Information accumulated at a weight list and used by the first phase of the Protocol.

Boudriga's approach (BA)

Boudriga et. al[27] suggested a new approach for building Intrusion tolerant MANETs. It consists of a Multi-level trust model and a network layer mechanism for resource allocation and recovery. The Multi-level trusts model supposes that the network is separated into two implicit sets: the resource's Domain and the user's Domain. Each resource allocates a distinctive trust level for each type of action that it is concerned with and each position where it emerges. Based on this trust level and on the movement, users or applications assign resources by a Distributed method. It assigns obtainable resources endeavoring to make the most of the use and reduce costs. For each application, only a portion of a resource is allocated at a given Node.

Data forwarding

Several works have planned secure Routing techniques to protect against numerous Attacks In spite Protocols guarantee the accuracy of the route discovery, they cannot ensure secure and undisrupted deliverance of Data. Clever Attackers can simply achieve unlawful access to the network, pursue the policy of the route discovery, place themselves on a route, and later transmit, drop or transform traffics, or insert Data Packets. Ina nutshell, an adversary can hide its malevolent performance for a phase of time and then Attack unpredictably, confusing its Detection. For these explanations, techniques to offer Data confidentiality, Data availability and Data integrity are essential for assurance secure Data forwarding. Numerous techniques have been planned for securing Data forwarding. Lightweight cryptographic techniques as Message verification Code (MAC) such as, are used to Data integrity. Nuglets, Friends and Foes, Sprite and others, recommend techniques to motivate node contribution In Data forwarding, demanding to ensure Data availability. CORE and CONFIDANT are examples of reputation systems that offer Information to differentiate among a reliable node and a malevolent Node. This Information also promotes Nodes to contribute In the network In Defense Line a reliable way. a number of solutions to offer Data confidentiality and Data availability have tried to affect procedures as redundancy and message protection to be further tough to Attacks. In SPREAD, SMT and SDMP, such as, the message are separated into multiple pieces by a message division algorithm. These pieces are concurrently mailed from the source to the Destination over multiple paths. In[28], a cross-layer approach is examined to progress Data confidentiality and Data availability, using directional antennas and intelligent Multi-path Routing with Data redundancy.

SPREAD

The Secure Protocol for Reliable Data Delivery (SPREAD) method offers the use of some methods to increase Data confidentiality and Data availability. at first, messages are divided into multiple pieces by the source Node, using the threshold secret sharing method. Each piece is encrypted and sent out via multiple sovereign paths. Encryption among neighboring Nodes with a dissimilar Key is understood In addition to the presence of an efficient Key management method. SPREAD spotlights on three major operations: to split the message, to select multiple paths and to assign message pieces into paths. Messages are split by the threshold secret sharing algorithm and each piece is allocated into a chosen path planning to reduce the likelihood of damage. SPREAD chooses multiple sovereign paths getting into account Security causes like the SPREAD is to attain an optimal share allocation way, where the Attacker should harm all the paths to get back the message.

SMT

The purpose of the secure message transmission (SMT) Protocol is to make sure Data confidentiality, Data integrity, and Data availability, protection the End-to-End communication against malevolent performance of intermediate Nodes. SMT utilizes four main characteristics: End-to-End secure and secure feedback mechanism, dispersion of the conveyed Data, instantaneous usage of multiple paths, and adaptation to the network changing circumstances. It needs a Security association (SA)[29] between the two ends communicating Nodes, so no link encryption is desirable. This trust association is essential for provided that Data integrity and verification of end Nodes, essential for any secure Communication method. The two end Nodes make use of a set of Node-disjoint paths, called Active Path Set (APS), being a subset of all presented paths connecting them. Data message is broken into numerous small pieces by the Information dispersal method[30]. Data redundancy is further to permit recovery, being also divided into pieces. All pieces are sending all the way through diverse routes existing In APS, increasing statistically the confidentiality and availability of exchanged messages. At the Destination, the dispersed message is effectively restructured only if an adequate number of pieces are acknowledged. Each piece transmits Message verification Code (MAC), permitting its integrity verification by the Destination. The Destination authenticates the inward pieces and acknowledged the effectively receive ones thought a feedback to the source. The feedback mechanism is also confined by cryptography and is dispersed

to offer fault Tolerance. Each path of APS has a reliability rate considered by the number of successful and unsuccessful transmissions on this path. SMT uses this rate to manage the paths In APS, demanding to decide and preserve a maximally secure path-set, and regulating its parameters to stay successful and efficient.

SDMP

The Secured Data Based Multi-path (SDMP) Protocol discovers also multiple paths among network Nodes to enhance the Robustness and Data confidentiality. The Protocol supposes Wired Equivalent Policy (WEP) link encryption/decryption of all the frames among neighboring Nodes, which offer link layer confidentiality and verification. SDMP can function with any Routing Protocol, which offers topology discovery and maintains the use of Multi-path for routing. SDMP differentiates between two types of path: signaling and Data. Signaling type needs only one path of the path-set existent between source and Destination Nodes, being the other paths available for Data transmission. The Protocol divides the message into pieces using the Diversity Coding approach [31]. The signaling path conveys all Information essential for message reconstruction at the Destination. Except the Attacker can achieve access to all of the conveyed parts, the possibility of message reconstruction is low. That is, to cooperate the confidentiality of the original message, the Attacker have to get inside snooping range of the source/Destination, or at the same time eavesdrop on all the paths used and decrypt the WEP encryption of each conveyed part. On the other hand, it is likely to assume parts

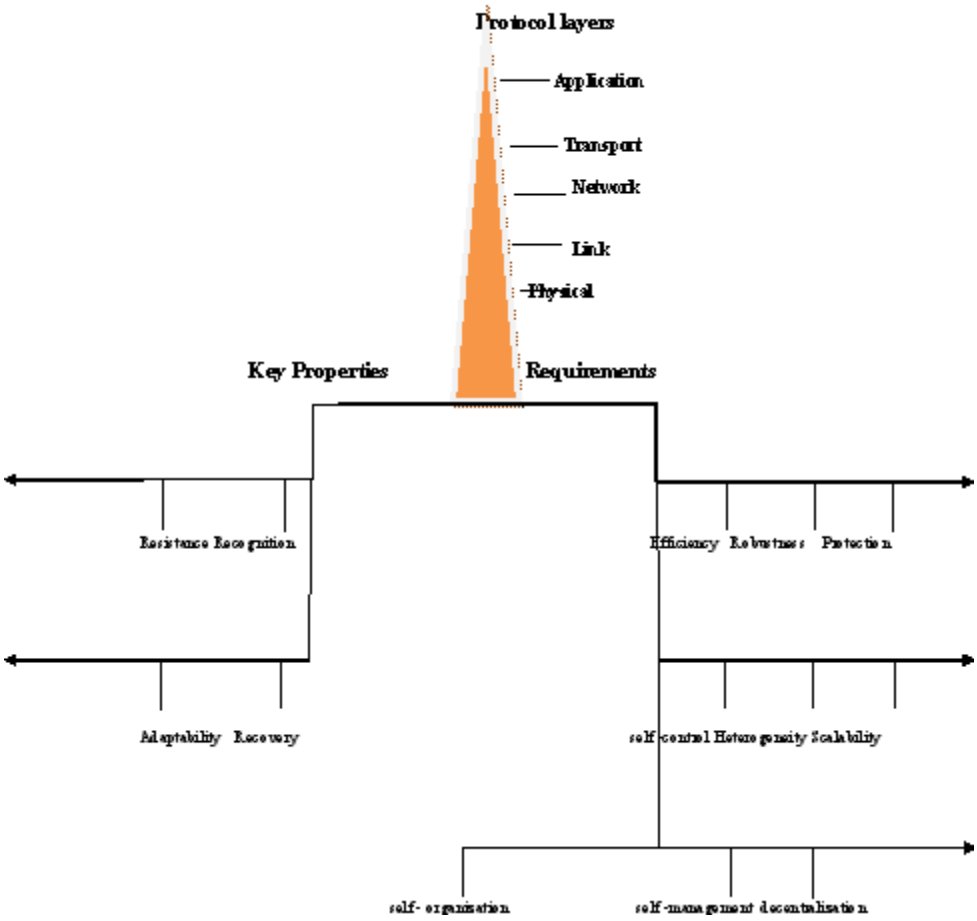

Fig. 5: Planes of view for Survivability

of the original message from only a few of the transmitted pieces, particularly as one piece of the original message is always sent In its original form on one of the paths.

Cross-Layer approach (CLA)

In compare to earlier solutions, a cross-Layer approach is examined In[28]. The solution uses directional antennas and intelligent Multi-path Routing to enhance End-to-End Data confidentiality and Data availability. Directional antennas make Eavesdropping more complex and reduce the area enclosed by Packet transmissions, reducing the overlap of message pieces conveyed by multiple paths. Thus, the use of directional antennas is acceptable by the decrease on the probability that and foe is capable to concurrently get together all of the message pieces at the source or Destination Nodes. A self-Adaptive transmission power Control mechanism is used mutually with directional antennas to decrease the message interception possibility. This mechanism permits the transmitter to use only sufficient transmission power In order to arrive at the intentional recipient, decreasing the radiation model for a given radio transmission and the likelihood of an Attacker to intercept the message transmission. Dynamically the transmission power is accustomed depending of the Data Packet type exchanged among neighboring Nodes. Multi-path Routing is also used. Thus, messages are divided Based are threshold secret sharing algorithm, and then the shares are sent by multiple Node-disjoint paths. Two intelligent Routing methods are planned to decrease message interception possibility. The previous decrease the physical distance of hops and the second decreases the path-set correlation factor.

Key management and access Control

Security solutions have depended on cryptography and assume the presence of an infrastructure for providing and managing keys. Some MANET's characteristics, as the deficiency of any central infrastructure, make Key management a challenge. In spite of this, Distributed and self-organized Key management System for MANETs have been planned. Fundamentally, there are two types of Key infrastructure. The second considers the public Key infrastructure, which offers a couple of keys (public / private) used for asymmetric cryptography, as In digital signatures. This subsection addresses the very relevant Survivable Key management Initiatives.

PGP -like (PL)

One of the Survivable Key management Initiatives for MANETs is called PGP -like[32]. This System handles the public Key management issue and suggests a completely Distributed self - Organizing public Key management infrastructure. PGP -like (PL) is based on the PGP functionality and each node is accountable for creating its public and private keys. Unlike PGP, where certificates are generally stored In centralized certificate repositories, certificates. In PGP System, Key verification is performed via chains of public - Key certificates. As a node itself produces public and private keys locally, public -Key certificates are issued Based on the presented trust between the Nodes. In this manner, if a node x considers that a given public Key belongs to a node z, then x can give public - Key certificate In which Kz is attached to z by the signature of x. primarily, each node grasps In its repository certificates issued by it and the certificates that other Nodes issued to it. PGP - like defines a mechanism that offers periodic exchanges of certificates between neighbor Nodes. This mechanism intends to allocate the certificates and turn into further efficient to discover a chain of public -Key certificates. In addition, techniques to keep informed and to invalidate keys are used to avoid inconsistency. PGP - like presents also functionalities to deal with misbehavior Nodes, like operations to crosscheck the keys In certificates and identify irregularity. The certificates are inconsistent when two or more of them are connected to the same user, but they present dissimilar keys or communicate the same public Key to dissimilar users.

Joshi's approach (JA)

Joshi *et. al.*, suggest a fully Distributed certificate authority method Based on secret sharing and redundancy[66]. In secret sharing mechanism, the certificate authority's private Key is first divided into parts. These parts or Key shares are then distributed among the Nodes In the network. To exchange Information, Nodes have to

remake the key. The certificate authority (CA) Key can be recreated by merging a smallest number of Key shares from the total number of shares. The number of Key shares per node is more than one by integrating redundancy into the network. As each node stores more than one Key share, then the number of Nodes important to recreate the CA Key is concentrated, increasing the probability of a lawful node for recreating the CA key. On the other hand, the redundancy creates a challenging as the probability of an intruder ingoing In the network and compromising the CA Key are enhanced. When an intruder accesses the network and compromises one Node, it becomes equivalent to a legitimate Node. To prevail over this issue, it is planned the use of an Intrusion Detection System (IDS), which should show the misbehavior/ compromised Nodes and remove them from the network.

URSA

URSA is a ubiquitous, decentralized, self - Controlled and robust access Control solution for Mobile ad-hoc Networks, where no single node dominates the access choice or is supposed to be totally confidence. As an alternative, multiple Nodes together monitor a local node and certify / revoke its ticket. Tickets execute the same functionality of conventional digital certificates, having expiration time, individual public Key of the Node, signature and identifier. They are certificated and updated periodically to oppose scheme of Attacks by multiple misbehavior Nodes. Certifications are based on RSA cryptosystem and on threshold cryptography- Based signature. URSA handles a localized group trust model where a node is measured trust if it is believed by a number of dependent Nodes. The trust relation is defining within definite period restricted by the ticket expiration time. Based on this model, trust Nodes can sign tickets for all other Nodes In the network. These Nodes also monitor other Nodes In order to identify probable misbehaviors. If a misbehavior node is identified, ticket revocation can be done to prevent the Attack propagation. Tickets are also periodically transformed to get better the toughness of the System.

Techniqal background

MANETs hosts will guaranteed and facilitate structure In infrastructure network s. Routing access Control and node Authentication are examples of network functionalities that will have to be executed by node collaboration. However, those hosts show characteristics, like constraints resources (processing, memory, Bandwidth, energy and other factors), bound their capability to perform intense actions and enlarge the complication on provided that network organization, control and security. Because of the communication type and constraints resources, MANETs are susceptible to miscellaneous types of attacks and intrusions.

Wireless communication is vulnerable to intrusions and interceptions. Probability will have made instruments or devices every time fewer, with resource restraints, and therefore simple objectives for overload attacks like In the paper securing ad-hoc network by Lidong Zhou[33]. The complete network decentralization, lack of supported infrastructure and dynamic topology boost the susceptibility to a lot of attacks like impersonation, Sybil[38], Selective forwarding, blackhole, wormhole[34-35].

Numerous explanations have been planned for Security troubles on Ad-hoc networks[35-37]. Inbroad-spectrum, these explanations affect preventive or reactive approaches by means of methods to defend fundamental Protocols. Basically, the clarifications use particular hardware, cryptographic primitives, mechanisms for overhearing communication or Protocols considered for the path diversity In Detection, Diagnosis And Isolation Of Control Attacks In Sensor network s by Issa Khalil, Saurabh Baqchi,Cristina Nitro-Rotaru[39]. Nevertheless, methods and mechanisms are used for a particular objective, being efficient In the given situation, but incompetent In other cases. Furthermore, every existing techniques and mechanisms are themselves unable of independently protecting beside the entire categories of attacks and instructions. Because of solutions limits and Manet's distinctiveness, Researchers have planned on scheming safety mechanisms for accomplishing network Survivability. Survivability is usually explained as the capability of a system to complete its mission or its job, Ina specific time,

In the existence of attacks, malfunctions or accident In Survivable network System: An Emerging Discipline[40]. The word system has a broad wisdom and might distinguish network s, way of communication or functions, and mission symbolizes the abstract goal and necessities of the system.

CONCLUSION

This paper observes Survivable approaches whose purpose is to facilitate network s to complete their functions properly and significantly even In the presence of Intrusions. In this paper we construct the very interrelated Survivable MANET ideas where either preventive or reactive techniques are combined implemented with tolerant technique. We categorize the defense lines getting into account Intrusion Tolerance techniques as well as classify Properties and needs of Survivability. The Initiatives are classified In three groups:

Discovery of Routing, Transmission 0f Data and Key management.

For each one, they are interrelated In terms of needs and Properties. The paper shows that Security solutions that still not yet discover related Survivability Properties and have only focused on one network layer or one type of Attack. The implementations, work and uses of MANETs have enhanced very much and, therefore, the Security problems and objective have turn out to be further significant. Conventional methods for security are not enough for such network s, as they present dissimilar characteristics and Properties that need new methods and techniques. This paper established Survivability concepts and its association with preventive, reactive and Tolerance defense lines. Survivable MANETs will be capable to accomplish their purposes and aims by means of the cooperation between those three defense lines. Key Properties of Survivability as resistance, acknowledgment, recovery and adaptability were thorough, and Survivability needs for MANETs were examined. Those necessities include self -Organization, self -Control, self -configuration, and self -management, access Control, protection, Authentication, scalability, redundancy and others. In addition, these Initiatives were explained emphasizing their Survivability needs and Properties. Based on this examination, we can bring to a close that (i) Security solutions for MANETs still be relevant a few set of preventive and reactive procedures; (ii) solutions focus either on Attacks or only one layer of the stack Protocol; (iii) adaptability Property is approximately unknown; (iv) needs as Heterogeneity, Efficiency, Robustness and self -management are not so far reached. In conclusion, this function highlights that a completely Survivable MANET be supposed to be appropriate cooperatively the three defense lines as an alternative of only one or two lines separately.

REFERENCES

1. http://seminarprojects.com/Thread-Mobile-adhoc-Network-MANET-fullreport#ixzz21Hmlyy36
2. http://seminarprojects.com/Thread-Mobile-adhoc-Network-MANET-fullreport?page=3#ixzz21HoJZJW0
3. http://seminarprojects.com/Thread-Mobile-adhoc-Network-MANET full report?page=3#ixzz21Hor7Oag.
4. http://seminarprojects.com/Thread-Mobile-adhoc-Network-MANET-fullreport?page=3#ixzz21Hp4OW
5. R. Ellison, D. Fisher R Linger, H Lipson, T. Longstaff and N Mead. Survivable Network system: An Emerging Discipline (cmu/sei-97-tr-013). Technical report, software Engineering Institute, Carnegie Mellon University, PA (1997)
6. B. Wu, J. Chen, J. Wu, and M. Cardei. wireless/Mobile network security, chapter A paperon Attacks and countermeasures In mobile Ad-hoc network s. Springer (2006).
7. P. E. Ver´yssimo, N. F. Neves, and M. P. Correia. Intrusion-Tolerant Architectures: Concepts and Design. Technical report DI-FCUL TR- 03-5, University of Lisbon, Department of informatics, University of

Lisbon ,portugal.

8. Y. Deswarte and D. Powell. Internet security: An Intrusion-Tolerance Approach. Proc. IEEE, **94**(2): 432-441 (2006).
9. R. Ellison, D. Fisher, R. Linger, H. Lipson, T. Long staff, and N . Mead, Survivable network system Discipline 013). Technical report, software Egineering Institute, University, Pittsburgh,.
10. J.-C. Laprie and B. Randell. Basic Concepts and Taxonomy of Dependable and Secure Computing. *IEEE Trans. Dependable security Computer*, **1**(1):11
11. I. Khalil, S. Bagchi, and C. Nita-Rotaru. DICAS: Detection, diagnosis and isolation of Control Attacks In sensor network s. InProc. International confrence on security and Privacy In Communication Networks (SECURECOMM), pages 89–100, Los Alamitos, CA, USA (2005). IEEE
12. A. Perrig, R. Canetti, J. D. Tygar, and D. Song. The TESLA Broadcast verification Protocol. *RSA Crypto Bytes*, **5**(2): (2002).
13. Y. Hu, D. Johnson, and A. Perrig. SEAD: Secure Efficient DistanceVector Routing for mobile wireless Ad-hoc Networks.
14. Y.-C. Hu, A. Perrig, and D. B. Johnson. Ariadne: A Secure On-Demand Routing Protocol for Ad-hoc Networks. wireless network s, **11**(1-2): 21
15. P. Papadimitratos and Z. Haas. Secure Routing for mobile ad hoc network s. InProc. Communication Networks and Distributed system Modeling and Simulation (CNDS) (2002).
16. P. Kotzanikolaou, R. Mavropodi, and C. Douligeris. Secure Multi-path Routing for mobile Ad-hoc network s. In Proc. Conf. wireless On-Demand network system and Services (WONS), pages 89–96, Washington, DC, USA (2005). IEEE Computer Societ.
17. S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating Routing misbehavior In mobile Ad-hoc Networks. In Proc. International Conf. Nobile Computing and networking (MobiCom), pages 255–265, New York, NY, USA, 2000. ACM Press.
18. L. Hu and D. Evans. Using directional antennas to prevent wormhole Attacks. In Proc. network and Distributed System security Symposium (NDSS), pages 89–96, Washington, DC, USA, 2004. IEEE
19. R. C. Linger, N. R. Mead, and H. F. Lipson. Needs definition for Survivable network system. In Proc. International confrence on Needs Engineering (ICRE), pages 00–14, Washington, DC, USA,
20. M. G. Zapata. Secure ad hoc on-demand distance vector routing.
21. S. Yi, P. Naldurg, and R. Kravets. security - aware Ad-hoc Routing for wireless network s. In Proc. ACM International Symposium on mobile Ad-hoc network ing & Computing (Mobi Hoc), pages 299–302, New York, NY, USA, 2001. ACM Press.
22. R. Ramanujan, S. Kudige, and T. Nguyen. procedures for Intrusion- resistant Ad-hocRouting algorithms TIARA. In DARPA Information Survivability confrence and Exposition (DISCEX), volume 02, pages 98–100, Los Alamitos, CA, USA, 2003. IEEE.
23. Y. Xue and K. Nahrstedt. Providing fault-tolerant Ad-hocRouting service Inadversarial environments. wireless Personal Communications: An International Journal, 29(3-4):367–388, 2004.
24. B. Awerbuch, R. Curtmola, D. Holmer, H. Rubens, and C. Nita- Rotaru. On the Survivability of Routing Protocols InAd-hoc wireless network s. InProc. International confrence on security and Privacy In Communication Networks (SECURE COMM), pages 327–338, Los Alamitos, CA, USA IEEE Computer Society (2005).
25. N. A. Boudriga and M. S. Obaidat. Fault and Intrusion Tolerance In wireless Ad-hocNetworks. InProc. IEEE wireless Communications and network ing confrence (WCNC), **4**: 2281–2286, Washington, DC, USA, IEEE (2005).
26. D. Holmer, C. Nita-Rotaru, and H. Rubens. ODSBR: An On-Demand Secure Byzantine Resilient Routing Protocol for wireless Ad-hocNetworks. To appear In ACM Trans. Information system security
27. N. A. Boudriga and M. S. Obaidat. Fault and Intrusion Tolerance In wireless Ad-hoc Networks. In Proc. IEEE wireless Communications and network ing confrence

(WCNC), volume 4, pages 2281–2286, Washington, DC, USA, IEEE (2005)

28. V. Berman and B. Mukherjee. Data security In MANETs using Multi-path Routing and directional transmission. InProc. IEEE international confrence on Communications (ICC), **5**: 2322–2328. IEEE Computer Society (2006).
29. D. Maughan, M. Schertler, M. Schneider, and J. Turner. Internet security association and Key management Protocol (ISAKMP). RFC 2408, Internet Engineering Task Force, (1998).
30. M. O. Rabin. Efficient dispersal of Information for security, load baLANcing, and fault Tolerance. *Journal ACM,* **36**(2): 335-348 (1989).
31. E. Ayanoglu, Chih-LInI, R. D. Gitlin, and J. E. Mazo. Diversity coding for transparent self - healing and fault-tolerant Communication Networks. IEEE Trans. Commun., **41**(11): 1677-1686 (1993).
32. S. Capkun, L. Buttyan, and J.-P. Hubaux. self -organized public - Key management for mobile Ad-hoc Networks. IEEE Trans. mobile Computing, **2**(1): 52–64 (2003).
33. L. Zhou and Z. J. Haas. Securing Ad-hoc Networks. *IEEE network* **13**(6): 24–30 (1999).
34. H. Yang, H. Luo, J. Kong, F. Ye, P. Zerfos, S. Lu, and L. Zhang. *Ad-hoc Network security: Challenges and Solutions*. CRC Press, (2004).
35. B. Wu, J. Chen, J. Wu, and M. Cardei. wireless / *mobile network security*, chapter A survey on attacks and countermeasures In mobile ad-hoc networks. Springer,2006
36. D. Djenouri, L. Khelladi, and A. N. Badache. A survey of security issues In mobile ad-hoc and sensor network s. *IEEE Commun. Surveys & Tutorials*, **7**(4): 2-28 (2005)
37. P. Argyroudis and D. O'Mahony. Secure routing for mobile ad-hocnetworks. *IEEECommun. Surveys & Tutorials*, 7(3):2–21, Third Quarter 2005.
38. J. Douceur. The sybil attack. In*Proc. International workshop on Peerto-Peer* system *(IPTPS)*, Cambridge, MA (USA), (2002).
39. I. Khalil, S. Bagchi, and C. Nita-Rotaru. DICAS: detection, diagnosis and isolation of control attacks In sensor network s. In*Proc. International confrence on security and Privacy In Communication network s (SECURECOMM)*, pages 89–100, Los Alamitos, CA, USA, 2005. IEEE Computer Society.
40. R. Ellison, D. Fisher, R. Linger, H. Lipson, T. Longstaff, and N. Mead. Survivable network system: An Emerging Discipline (cmu/sei-97-tr-013). Technical report, software Engineering Institute, Carnegie Mellon University,PA (1997).