www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 4 April, 2013 Page No. 1063 -1071

Improved Security Architecture For Up Keeping Routing Services on Ad Hoc Networks

Regan. R[1], Ilakkiya Veera[2], Kousalya.J[3]
[1,2,3]Department of Computer Science and Engineering
University College of Engineering, Panruti
[1]reganr85@gmail.com, [2]veera220692@gmail.com,[3]kowse726@gmail.com

Abstract

Nowadays People's dependence is increasing on crucial applications and wireless networks for executing anytime and anywhere. The presence of active routing protocols enable ad hoc network forming quickly. WANETs suffer from security attacks and intrusions even under several defense mechanisms. In case of providing both secure options and network procedures, we present SAMNAR, a Survivable Ad hoc and Mesh Network Architecture. Its objective is to provide essential preventive, reactive and tolerant security structures adaptively under damages and disturbances. The purpose of SAMNAR is to design a path selection scheme for Wireless Ad hoc Network routing. Our outcome explains that survivability achieved on routing services even under several damages and intrusions.

Index Terms-Security Architecture, Intrusions, Routing, Survival path, Performance.

I.Introduction

Our society depends on a wide variety of telecommunication services to support our demands for everything from pure entertainment to commerce, banking and life critical services. A variety of threats, like attacks, accidents, and failures, may cause minor or major service degradations in the telecommunication services and network. Self-organizing wireless networks, as ad hoc, mesh and sensor networks, request simultaneously high level of reliability, availability and security. These networks have increased the dependence of people on applications available on portable devices and supported by wireless communication.

Mobile applications, such as those on commercial, financial and medical fields, mandate a predictable and acceptable network operation, guaranteeing data integrity, confidentiality and non-repudiation. Hence, self-organizing wireless networks must be survivable to attack and intrusion events. Survivability means the network capability of maintaining its essential services, as link-layer connectivity, routing and end-to-end communication, even under faults, attacks or intrusions [1].

Security is a challenge for self-organizing wireless networks. Several threats take advantage of protocol faults and vulnerabilities on operating systems of devices, as well as network characteristics. These networks are supported by shared wireless medium, highly dynamic network topology, multi-hop communication and low physical protection of portable devices [2]. These characteristics make self organizing wireless networks prone to interferences, interruptions and misbehaviors, compromising easily network services. Different security solutions have been proposed in the literature [2–4]. They apply preventive, reactive and tolerant security mechanisms. However, these mechanisms are not enough to put all attacks and intrusions off when applied separately. Preventive solutions attempt to thwart attacks by cryptography, authentication and access control mechanisms. They are vulnerable to malicious nodes that already participate in network operations.

Reactive solutions, such as intrusion detection systems or reputations systems, seek to

detect intrusions and react accordingly [5]. These solutions work efficiently only against well-known attacks or intrusions. Tolerant solutions focus on mitigating the impact of attacks using fault-tolerant techniques, typically redundancy and recovery mechanisms. However, these solutions remain still focused on one specific issue or particular layer of the protocol stack, being ineffective to ensure essential services.

In this article we address the problem of providing survivability in self-organizing wireless networks. We present SAMNAR, a conceptual architecture to maintain the operation of essential network services on an acceptable level even in face of faults, attacks or intrusions. The SAMNAR architecture is inspired on the human body immune system and proposes a new approach to security management. SAMNAR employs preventive, reactive and tolerant defense lines and manages them in a cooperative and adaptive way. SAMNAR also considers information from the environment and from different layers of the protocol stack to take accurate decisions. We develop a security and performance framework based on the SAMNAR architecture.

Ii.Related Work

This section starts giving an overview of existing security management architectures for network survivability and it finishes presenting related works to route selection.

A. Security Management Architecture

In these last few years, research interests in survivability have increased. Initially addressed by military area, the first survivability architectures have been proposed in order to improve both security and dependability of information systems, distributed services and storage systems in the Internet domain [6–8]. Although the importance of all architectures in the survivability development, we emphasize Willow [8], SITAR [7] and SABER [6] architectures due to their completeness in terms of survivability properties.

The Willow architecture [8] is designed to enhance the survivability of critical information systems. This architecture proposes the merging of different mechanisms aiming to avoid, eliminate and tolerate faults. All of these mechanisms are based on a reconfiguration approach in which nodes of the network can together monitor and respond to faults. Each node and network operations are monitored continuously. However, the analysis of their operation is performed by central nodes, called servers, restricting the efficiency of the architecture.

SITAR [7] is a survivable architecture for distributed services whose goal is to provide the minimal level of services despite the presence of attacks. This architecture comprises different components such as proxy servers, monitors, audit control module and adaptive regeneration module. These components are transparent for the clients and servers of the service and each component has a backup in order to guarantee its operation. The architecture controls all requests and responses, and can be centralized or partially distributed.

The SABER architecture [6] integrates also different mechanisms to improve the survivability of Internet services. SABER proposes a multi-layer approach in order to block, evade and react to a variety of attacks in an automated and coordinated fashion. The SABER architecture is composed of a Denial of Service (DoS) resistant module, an Intrusion Detection System (IDS), a migration process and an automated soft-patching system. All of these components are controlled by an infrastructure of coordination. This infrastructure provides the communication and correlation among the components in a decentralized fashion.

B.Secure Path Selection Approaches

Since routing is an essential service for WANETs, researchers have actively explored many mechanisms for enhancing routing protocols by techniques of redundancy and security approaches. Some of them emphasized the importance of the path selection phase, proposing approaches to improve it. Those approaches can be broadly grouped into two classes, single

criterion based and multi-criteria based, where just a minority of them employ security characteristics as selection criterion. Moreover, to the best of our knowledge, none of them address network survivability. Split multipath routing protocol (SMR) [12], for example, picks out the shortest routing path as the primary route, and then computes the maximum disjointed path, as a secondary route.

Disjoint path set selection protocol (DPSP) [11] chooses in linear time a set of highly reliable paths, determined by the path length. Genetic Fuzzy Multi-path Routing Protocol (GFMRP) [13] is the most relevant protocol that focuses on these issues. There, Liu *et. al*apply fuzzy set theory and evolutionary computing to correlate criteria and select a set of paths. Fuzzy logic is applied to minimize correlation complexity.

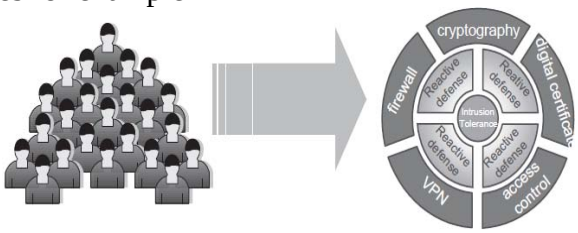
However, GFMRP's goal is to maximize network lifetime and reliability.

Yi *et. al*proposed SAR (security-aware ad hoc routing) [6], [13]. It classifies nodes based on their trust level. In the route discovery process, the source node can estimate the minimum security level required by node to participate in the routing path. However, SAR is not a multipath routing and does not correlate security criteria with other related to network characteristics. Nie*et. al*proposed the fuzzy logic based security-level (FLSL) routing protocol. It selects the highest security-level routes, calculated by fuzzy logic through the correlation among path length and two security characteristics, cryptographic key length and frequency of key exchanges.

However, the initial FLSL proposal defines a single path protocol and it does not address survivability issues.

Inspired by the immune system of the human body, we argue that network survivability can be reached by the cooperative and adaptive use of preventive, reactive and tolerant defense lines. Figure illustrates our survivable approach. It consists of different levels of obstacles, that must work together in an adaptive way, against attack and intrusion events.

The first obstacle is generated by preventive security mechanisms aiming to avoid any type of attack. Examples of these mechanisms are firewalls and cryptography. They block certain attacks, but naturally will be incapable of preventing others due to Attacks Defenses for example



their limitations. Cryptography and firewall,are vulnerable to attacks produced by nodes already legally participating in the network.

For some attacks succeeding to intrude into a node or network, reactive defenses will try to detect and react against them. Mechanisms such as intrusion detection systems or reputation systems intend to evaluate the behavior of nodes in the network. However, reactive defenses work efficiently against well-known intrusions, being vulnerable to unknown intrusions. IDSs, for example, require extensive evidence gathering and comprehensive analysis in order to detect intrusions based on anomalies or predetermined intrusion patterns.

The use of only one route selection criterion ignores many WANET characteristics. MANETs, for example, presents dynamic topology determined by different factors such as node mobility, signal strength, node battery capacity, among others. Therefore, reactive defenses also present limitations. Some intruders can be successful in compromising the network. In order to guarantee the operation of essential services, intrusion tolerance techniques have been applied [10]. These techniques aim to mitigate intrusion effects, and stimulate preventive and reactive defenses to adapt against attacks or intrusions.

Iii.Experimental Work

This section covers the description of SAMNAR and the selection of most survival path using this architecture.

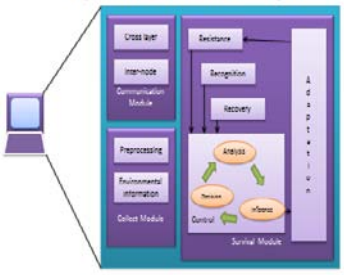
A.The SAMNAR architecture:

The SAMNAR, Survivable Ad hoc and Mesh Network ARchitecture, is inspired from the human body immune system. It states modern security management method by the adaptive coordination of preventive, reactive and tolerant defense lines. Preventive defense lines comprise security mechanisms attempting to avoid attacks,

such as cryptography, firewalls and access control techniques. Reactive defenses try to detect and react against intrusions by security mechanisms, such as reputation systems and intrusion detection systems. Tolerant defenses aim to mitigate damages caused by attacks or intrusions, and recover compromised services. Redundancy is one of the techniques employed to reach recovery.

SAMNAR focuses on up keeping the improvement of necessary services, as link-layer connectivity, routing and end to end communication. It establishes three integrated modules. Fig. 1 illustrates these modules.

Figure1:SAMNAR architecture - Diagram



Each node/device in the network independently implements and performs these three modules, optimizing them to consider its resource limitations. The survival module includes the five independent components. Four of them are related to resistance, recognition, recovery and adaptability, and the last one is the control component. These properties represent, respectively, the network capability of repelling attacks; detecting attacks and evaluating the extent of damage; restoring disrupted information or functionalities; and quickly incorporating lessons learned from failures and, thus, adapting to emerging threats.

The resistance component employs preventive mechanisms, such as firewall, access control, authentication and cryptography. This component works in a self-protection and self – adjusting fashion where preventive mechanisms and their configuration will be changed depending on the network or environment conditions. The rule of a distributed firewall, for instance, can be more rigorous in certain environments, while simpler rules can be applied in more secure environments. Another example is the cryptographic key size used that can be larger depending on the environment or network condition. The recognition component comprehends reactive mechanisms to identify malicious behaviors, such as IDSs, reputation systems, anti-malwares and anti-spammers. All the mechanisms selected will be reconfigured if necessary by the adaptation component. New configurations on the fly, such as IDS rules, depend on the network and environment conditions. Also, this component provides information about detections, trustworthiness of neighbor devices, among others to the control component. The recovery component consists of mechanisms to enhance the attack tolerance of network essential services. For example, the use of two cryptography algorithms successively and the replication of message pieces. Sending redundant message pieces by different routes increases the probability of the message to be received by the destination node and the possibility of message recovery in case of piece losses.

The adaptation component complements the previous ones. It can make the replacement of a given protocol or a defense mechanism, such as changing a weaker cryptographic algorithm for a stronger one, depending on the requirements on time. Further, this component can change the key size of a cryptographic algorithm, the rules into an IDS or a firewall, the used route and others in accordance with the network condition or decisions taken by the control component. The control component manages and coordinates all modules in the architecture. It receives information from communication and collect modules as well as from the resistance, recognition and recovery components. Adaptation component learns with taken actions and later, it can take the same action if the node or network presents a similar condition.

The communication module is responsible for cross-layer and inter-node communications. The inter-layer component offers the exchange of inter-layer information. The internodecomponent provides the communication, exchange and synchronization of information among the nodes aiming to guarantee the survivability of the whole network. The collect module holds mechanisms to gather all data required by the survival module. This module is composed of the preprocessing and environmental information components. The first one is exploited when gathered data need to be

processed before sending to the survival module. Normalizations, previous calculations and others are examples of preprocessing used to facilitate analyses and inferences of the survival module. The second component stores information gathered periodically about the network conditions, sending it to the survival module when required.

B. Survival path selection scheme:

The proposed path selection scheme aims at determining routes that can guarantee the routing service even under attacks or intrusions. The path selection scheme is a multi-criteria based scheme employing both conventional criteria and security criteria to point out the most survivable paths. Defense mechanisms support security criteria, being certificate expiration time and cryptographic keylength, criteria from preventive defenses; node reputation, from reactive defense; and path degree, criterion representing tolerance. More security criteria could also be employed, such as the type of cryptography and the percentage of false positive or false negative.

Conventional criteria support the resource and performance management and, in this case, we employ remaining energy (energy rate) and path length as network information (environmental information), although other criteria could be used, as path throughput or link stability. Defense mechanisms support security criteria, being certificate expiration time and cryptographic keylength, criteria from preventive defenses; node reputation, from reactive defense; and path degree, criterion representing tolerance. More security criteria could also be employed, such as the type of cryptography and the percentage of false positive or false negative. We highlight that multi criteria based schemes consider better WANET characteristics leading to more accurate choices. Example of using multi-criteria approach for path selection is the Genetic Fuzzy Multi-path Routing Protocol (GFMRP) [29] protocol. For that protocol, Liu *et. al*apply fuzzy set theory and evolutionary computing to correlate criteria and select a set of paths. Fuzzy logic was applied to minimize correlation complexity. However, GFMRP's goal is to maximize network lifetime and reliability. As GFMRP, few other multi-criteria protocols were proposed [30], [31], however they do not take into account security aspects. Fig. 2 illustrates the correlation between the SAMNAR architecture and its instance, the survival path selection scheme.

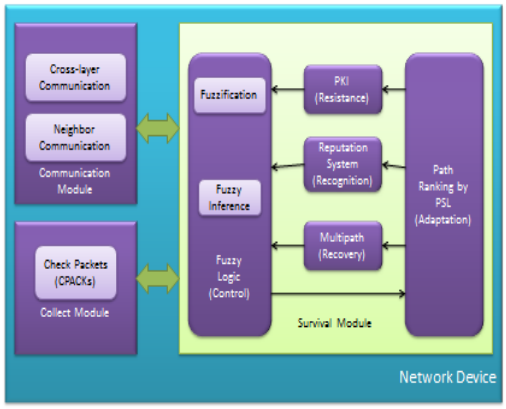
Survival module:

Each component of the survival module (resistance, recognition, recovery, adaptation and control) is specified for the path selection scheme.The resistance component consists of a public key infrastructure that

Supports cryptographic operations and

digital certifications.

Figure2: Survival path selection scheme - diagram



The recognition component is composed of a reputation system, and a multipath routing protocol provides the properties required by the recovery component. The adaption and control path ranking. The path selection scheme employs fuzzy components comprise fuzzification, fuzzy inference and logic (FL) as control component, because it is a multi-valued logic, allowing the definition of intermediate values between conventional measures, like true or false.

The control component calculates a path survivability level (PSL) for each route following the FL stages: input fuzzification and inference. Based on PSL, the adaptation component ranks paths, being the most survivable route chosen for data transmission. However, the PSL value can change with criterion updates resulted from new data collections. However, the PSL value can change with criterion updates resulted from new data collections. Thus, the set of selected routes can also adaptively change. The adaptation capability implemented in the path selection scheme consists in choosing the most appropriate route to be used considering the network conditions. Fuzzy inference process maps inputs

to outputs by rules following the form if-then. Inputs and outputs values lie in
fuzzy sets into the interval [0.0,1.0], in which 0.0 means absolute falseness and 1.0 means absolute truth. The set of rules composes the knowledge base of the scheme, generating outputs in order to make decisions. Path survivability levels are estimated by fuzzy inference process.

1) **Fuzzification***:* Fuzzy rules manipulate values in then fuzzy interval from 0.0 and 1.0, even if input values lie in different intervals. Conventional and security criteria values are represented by linguistic terms as "strong", "weak", "large", "small", among others. Each criterion has a set of linguistic values, which are mapped to fuzzy interval by membership functions. This process is called *fuzzification*. It follows trapezoidal functions since they have been extensively used in real-time applications due to their simple formulas and computational efficiency. Distinct and independent conditions, represented by conventional criteria, affect differently path survivability level. Remaining energy, for example, impacts on survivability since nodes with higher energy rate can participate in the path by a longer time period enhancing path stability. Stable paths are preferred for decreasing the number of route discoveries caused by path breaks. Route discoveries enable the participation of new malicious nodes in routes, reducing the probability of survivability. Further, paths with high remaining energy can tolerate overload attacks, improving the survivability level. Remaining energy is represented by the following linguistic terms: *low*, *medium* and *high*. Fuzzy inference considers the remaining energy of each path (*Ei*), estimated by the minimum value among the rates of all *n* nodes in the path *i*. Thus:

$$Ei = min(Ei1, Ei2, \ldots, Ein) \quad (1)$$

Path length (L) denotes the number of intermediate hops between the source node and the destination node. Higher path length results in lower performance. For security, higher path length raises the probability of existing malicious nodes in the path. Thus, shorter paths are preferred than longer ones. Path length variable has three fuzzy sets: *short*, *medium* and *long*. Based on results of for the average path length, paths with 1 or 2 hops are considered short, paths with 2, 3, 4, 5 and 6 are considered medium, and paths with more than 6 intermediate hops are considered long. Security mechanisms generate security criteria values which are used for taking decisions. Certificate expiration time (T), for example, presents two fuzzy sets, *imminent* and *far*. If the certificate expires within 10s or less, it is imminent, and far when it expires within 60s or more. These values were chosen based on results found in [14], in which they argue that the majority of path durations lie in the interval of 10 and 20 seconds. Expiration time smaller than path duration enhances the likelihood of the certificate to be compromised due to updates when the path is still alive. Thus, more imminent certificate expiration time reduces the survivability level and this criterion represents preventive defense lines.

For cryptographic key length (K), two fuzzy sets are defined, *short* and *long*, as in [16]. If the secret key has 40 bits or less, it is considered short, and it is long with 128 bits or more. Longer key lengths make cryptographic mechanisms more resistant to attacks. Thus, the survivability level is directly proportional to the key length. The reputation (R) of a path i is the lowest node reputation value in the path. Considering the existence of a reputation system in the network that generates values in the interval between 0.0 and 1.0 to indicate node behavior, the path reputation linguistic variable owns two fuzzy sets, *good* or *bad*. Path with higher good reputation values are preferred. Good reputations are those with values equal or higher than 0.8. The reputation of the path with *n* nodes is calculated as:

$$Ri = min(Ri1, Ri2, \ldots, Rin) \quad (2)$$

Path degree (D) represents tolerant defense lines, being defined by the minimum node degree among all *n* nodes. participating in a path *i* (Eq. 3). The node degree is defined by the number of its direct neighbors. Higher neighbor number augments the probability of finding redundant or alternative paths, and thus can improve the tolerance and survivability.

Path degree linguistic variable has three fuzzy sets: *few*, *normal* and *many*. Fig. 5 presents the membership function for this linguistic variable.

$$Di = min(Di1, Di2, \ldots, Din) \quad (3)$$

The fuzzy logic inference results in the path survivability level (*PSL*). Knowing the independence among the six criteria, their relation with PSL follows the Eq. 4:

$$PSL \propto E \cdot K \cdot R \cdot D \cdot 1/L \cdot 1/T \quad (4)$$

Only for exemplifying the importance of security criteria and their impact in order to make decision on PSL.note that with *L* up to 5, *L* is not an important factor to improve the PSL, being *K* more than 50 the main factor. However, for *L* higher than 5, both *L* and *K* improve the PSL, although it only achieves 0.45. As defined in Eq. 4, PSL is minimized by high values of *L*. It is also important to mention that the fuzzy sets of *E*, *K*, *R*, *D*, *L* and *T* are predetermined based on values analyzed on
the literature. Fuzzy sets are not adapted along the execution of the path selection scheme. Only the used path can be adapted in accordance to network conditions.

2) **Fuzzy inference and path ranking:** Fuzzy inference follows fuzzy rules composed of fuzzy sets. In our case, Larsen's max-product inference mechanisms [15] calculate the path survivability level. For each linguistic variable, their values on fuzzy set are combined by means of algebraic product operation. Next, the highest PSL value is chosen by the adaptation component for data transmission. The adaptation component ranks each path by its PSL, choosing the path with the highest PSL. The selected path is used until it is broken or until a new data collection phase occurs. If the path is broken before that, the next path with higher PSL is used. If a new data collection phase finishes and values change the path ranking, the source and destination nodes will use the most survival path. This process allows the self-adaptation of routing higher PSL is used. If a new data collection phase finishes and values change the path ranking, the source and destination nodes will use the most survival path. This process allows the self-adaptation of routing on network changes.

Collect and communication module:

In order to collect data periodically, special packets, called check packets (CPACKs), are sent. Each CPACK owns a cryptographic message digest generated by a hash function to prevent forgeries. After generating the message digest, nodes send check packets for all paths the node knows. The route discovery process follows the specification of the routing protocol being independent of the path selection scheme. Routes associate a source to a destination node, being data collections initialized by source nodes. CPACKs are forwarded hop by hop to the destination and, in each intermediate nodes, CPACKs gather criteria values and store them on specific fields.Arriving at the destination node, it sends the packet back. The packet can use any route to return to the source. A CPACK owns eight main fields: *destination IP address*, *source IP address*, *way*, *energy rate*, *reputation*, *validation*, *path degree* and *hop*. Source and destination addresses assist the packet routing and the field "way" indicates if CPACK is going to or coming back from the destination node.If "way" value is 0, it is going to destination node and collects data.If "way" value is 1, the packet is just forwarded, without gathering data.

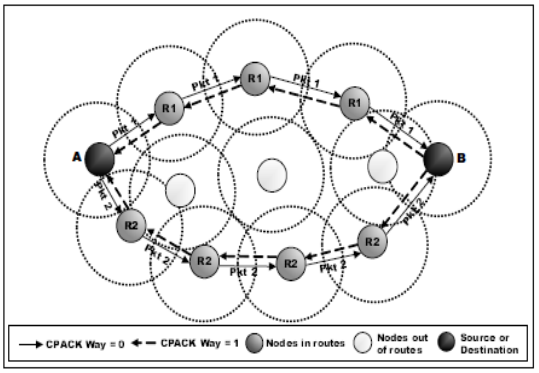


Figure 3: Data collection phase

"Energy rate", "reputation", "validation" and "path degree" fields store, respectively, the smallest value of remaining energy, collection phase, where a source node (node A) has previously discovered two routes, R1 and R2, to achieve the destination node (node B).

These routes have been found by the discovery phase of the routing protocol, being independent of the scheme proposed in this work. For data collection, two check packets, *Pkt*1 and *Pkt*2, are sent from node A to node B by routes R1 and R2, respectively. When these packets are going towards node B they collect data. Arriving at node B, these packets are sent back to node A, disabling their capability to collect data. The time interval between a data collection process and another is equal to *x* seconds. After each data collection process, source node calculates the survivability level for each path (PSL).

Algorithm:

For data collection:

1. Source node sends CPACKs to destination node.

2. Nodes in path entries criteria values in CPACKs.

Conventional Criteria:

4. Path Length (L)

L=intermediate nodes between source and destination.

5. Energy Rate (E)

$E= \min (E1^i, E2^i, \ldots, En^i)$

Security Criteria:

Preventive mechanisms:

6. Certificate Expiration Time (T)

If T<10s entry imminent

Else if T>=60s entry far

7. Cryptographic Key Length (K)

If K<40b entry short

Else if K>=128b entry long

Reactive mechanisms:

8. Node Reputation (R)

$R= \min (R1^i, R2^i, \ldots, Rn^i)$

Tolerant mechanisms:

9. Path Degree (D)

$D= \min (D1^i, D2^i, \ldots, Dn^i)$

10. After data collection source calculates PSL.

$PSL \propto E \bullet K \bullet R \bullet D \bullet 1/L \bullet 1/T$

11. Then source Ranks paths based PSL.

12. Highest PSL path selected for data transmission

IV. RESULTS AND DISCUSSION

This article presented SAMNAR, a conceptual architecture for security management in self-organizing wireless networks. SAMNAR is inspired on the human body immune system and provides survivability of essential network services. The architecture comprises three main modules, survival communication and collectmodules. We have designed a framework for security and performance management, where each SAMNAR's module is developed. We offer some research directions highlighting main issues for each functional block proposed in the framework in order to guide future works.

V.REFERENCES

[1] P. E. Heegaard and K. S. Trivedi, "Network survivability modeling," Computer Networks, vol. 53, no. 8, pp. 1215–1234, 2009.

[2] F. Martignon, S. Paris, and A. Capone, "Design and implementation of MobiSEC: a complete security architecture for wireless mesh networks," Computer Networks, vol. 53, no. 12, pp. 2192–2207, 2009.

[3] J. Dong, K. Ackermann, and C. Nita-Rotaru, "Secure group comm.In wireless mesh networks," Ad Hoc Networks, vol. 7, no. 8, pp. 1563–1576, 2009.

[4] Y. Yuan, S. Wong, S. Lu, and W. Arbaugh, "ROMER: resilient opportunistic mesh routing for wireless mesh networks," in IEEE WiMesh, 2005.

[5] I. Akyildiz and X. Wang, "A survey on wireless mesh networks," IEEE Communication Magazine, vol. 43, no. 9, pp. 23–30, 2005.

[6] A. Keromytis, J. Parekh, P. N. Gross, G. Kaiser, V. Misra, J. Nieh, D. Rubenstein, and S. Stolfo, "A holistic approach to service survivability," in ACM SSRS. New York, NY, USA: ACM, 2003, pp. 11–22.

[7] F. Wang and R. Upppalli, "SITAR: a scalable intrusion-tolerant architecture for distributed services," in DISCEX, vol. 2, 2003, pp. 153–155.

[8] J. Wylie, M. Bigrigg, J. Strunk, G. Ganger, H. Kili¸c¸c¨ote, and P. Khosla,
"Survivable information storage systems," IEEE Computer, vol. 33, no. 8, pp. 61–68, 2000.

[9] S. Yi, P. Naldurg, and R. Kravets, "Security-aware ad hoc routing for wireless networks," in *Proc. 2001 ACM MobiHoc*, pp. 299–302.

[10] Y. Qian, K. Lu, and D. Tipper, "A design for secure and survivable wireless sensor networks," IEEE Wireless Communications, vol. 14, no. 5, pp. 30–37, 2007.

[11] P. Papadimitratos, Z. J. Haas, and E. G. Sirer, "Path set selection in mobile ad hoc networks," in *Proc. 2002 ACM MobiHoc*, pp. 1–11.

[12] S. Lee and M. Gerla, "Split multipath routing with maximally disjoint paths in ad hoc networks," in *Proc. 2001 IEEE ICC*, pp. 3201–3205.

[13] H. Liu, J. Li, Y.-Q. Zhang, and Y. Pan, "An adaptive genetic fuzzy multi-path routing protocol for wireless ad hoc networks," in *Proc. 2005SNPD/SAWN*, pp. 468–475.

[14] Y. Han, R. J. La, A. M. Makowski, and S. Lee, "Distribution of path durations in mobile ad-hoc networks: Palm's theorem to the rescue,"

Computer Networks, vol. 50, no. 12, pp. 1887–1900, 2006.
[15] L. A. Zadeh, "Fuzzy logic," Computer, vol. 21, no. 4, pp. 83–93, 1988.
[16]J. Nie, J. Wen, J. Luo, X. He, and Z. Zhou, "An adaptive fuzzy logic based secure routing protocol in mobile ad hoc networks," *Fuzzy Setsand Systems*, vol. 157, no. 12, pp. 1704–1712, 2006.