ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 11, November 2014

Secure Path Selection Using SAODV in Wireless Ad Hoc Network

Arya.S.P

Abstract: Due to the raising dependence of people on critical applications and wireless networks, high level of reliability, security and availability is claimed to assure secure and reliable service operation. Wireless ad hoc networks (WANETs) experience serious security issues even when solutions employ preventive or reactive security mechanisms. In order to support both network operations and security requirements of critical applications, we present SAMNAR, a Survivable Ad hoc and Mesh Network ARchitecture. Its goal lies in managing adaptively preventive, reactive and tolerant security mechanisms to provide essential services even under attacks, intrusions or failures. We use SAMNAR to design a path selection scheme for WANET routing. The evaluation of this path selection scheme considers scenarios using urban mesh network mobility with urban propagation models, and also random way point mobility with two-ray ground propagation models. Results show the survivability achieved on routing service under different conditions and attacks**.**

Keywords: Security Management, Wireless Adhoc Networks, Survivability, Routing

I.INTRODUCTION

Recent technological advances in wireless networking have popularized the use of portable devices, raising the dependence of people on them for executing anywhere and anytime critical applications, like business-critical applications in financial transactions or life-critical applications in healthcare. Such dependence claims simultaneously for high level of reliability, security and availability to assure both secure and reliable service operation even under failures, intentional threats or accidents. Wireless ad hoc networks (WANETs) mobile or stationary – have envisioned to support ubiquitous computer connectivity by self-organized portable devices, (nodes), communicating among themselves in a wireless and multi-hop fashion.WANETs, such as mobile ad hoc networks (MANETs) or wireless mesh networks (WMNs), experience serious security problems due to their particular characteristics. Wireless communication can endure interferences or malicious interceptions, whereas multi-hop communication assumes that each node will perform properly its functions to support network services. Further, self-organization increases the complexity of security management operations as access control, node authentication, secure routing and solutions for WANETs employ preventive or reactive security mechanisms. Each security mechanism addresses specific issues having limitations to cope with different type of attacks and intrusions. Security management lies in one of the key research challenges on WANETs due to their characteristics, critical application requirements and restrictions on defense lines. Security management consists of mechanisms to control security mechanisms and services, thwarting attacks or intrusions. In this work, introduce SAMNAR, a Survivable Ad hoc and Mesh Network ARchitecture, whose goal is the design of survivable essential network services against attacks and intrusions. SAMNAR manages preventive, reactive and tolerant security mechanisms in an adaptive and coordinated way, focusing on the survivability of link-layer connectivity, routing and end-to end communication. SAMNAR supporting the development of a survival path selection scheme on routing service.

II. RELATED WORK

A. Security management architectures to network survivability

Initially, the architectures for network survivability were proposed to improve both security and dependability of information systems in the Internet context. The importance of all architectures to support the survivability concept, highlight SABER and SITAR architectures due to their completeness in terms of survivability properties as resistance, recognition, recovery and adaptation. SITAR is architecture for surviving distributed services and comprises different components. SITAR coordinates all components and controls any request or response in a centralized or partially distributed way. The SABER architecture integrates also different security mechanisms to improve the survivability of Internet services. Its components, as DoS resistant module, IDS and anomaly detection, migration process and automated soft-patching system, are controlled by a coordinated infrastructure providing the communication and correlation among the components in a decentralized fashion. In a security management architecture towards a survivable access control in WANETs is proposed, being the survivability achieved by the creation of secure groups.

B. Secure path selection approaches

Routing is an essential service for WANETs, researchers have actively explored many mechanisms for enhancing routing protocols by techniques of redundancy and security approaches. The criterion is generally a network

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 11, November 2014

characteristic, representing its state or a node condition. Split multipath routing protocol (SMR), picks out the shortest routing path as the primary route, and then computes the maximum disjointed path, as a secondary route. Genetic Fuzzy Multi-path Routing Protocol (GFMRP) is the most relevant protocol that focuses on these issues. There, apply fuzzy set theory and evolutionary computing to correlate criteria and select as set of paths. However, GFMRP's goal is to maximize network lifetime and reliability. Awerbuch proposed a new algorithm for adaptively selecting routing paths in a network with dynamic adversarial edge failures. Nevertheless, the path selection is made comparing accumulated packet loss on all paths. Yi proposed SAR (security-aware ad hoc routing) . 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 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.

III. SYSTEM MODEL AND ASSUMPTIONS

A. Network model

This work addresses multihop wireless ad hoc networks composed of mobile or stationary nodes. All nodes in the WANET are connected through bidirectional wireless links and are equipped with IEEE 802.11 radios. The existence of independent paths between source and destination nodes increases the routing tolerance against attackers in specific paths. Hence, a multipath node-disjoint routing protocol is also expected. The routing protocol supports the proposed scheme to attain its goals: (i) to decrease the probability of malicious nodes to compromise an entire set of available paths between a pair of nodes; and (ii) to assist adaptations on the routing protocol, selecting the best paths in terms of performance and security.

B. Attack model

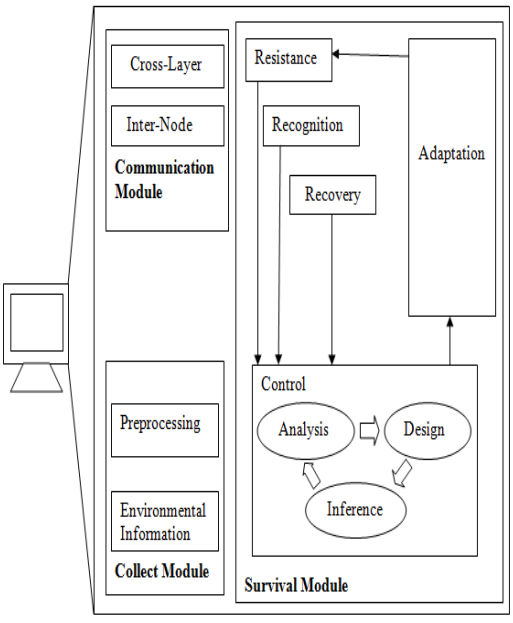
Different types of attacks can harm WANETs. This work focuses on attacks that can compromise the availability of network operations due to their challenging features. It is considered attack scenarios in which malicious node's actions can deny or delay WANET services. Particularly, this work handles variations of DoS attacks, as grayhole (also selective packet dropping), blackhole and sinkhole attacks.

C. Security model

We assume the existence of at least one preventive, reactive and tolerant security mechanism on the network. Preventive defenses comprise security mechanisms that attempt to prevent attacks, such as cryptography, firewalls and access control techniques. Reactive defenses, such as reputation systems and intrusions and intrusion detection systems, try to detect or to indicate intrusions and misbehaving nodes, offering to the network the possibility of reacting against them. Tolerant defenses aim to mitigate damages caused by attacks or intrusions, and recover compromised services

IV. THE SAMNAR ARCHITECTURE

The SAMNAR, Survivable Ad hoc and Mesh Network ARchitecture, is inspired on the human body immune system. It defines a new security management approach 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. modules. Each node/device in the network independently implements and performs these three modules, optimizing them to consider its resource limitations. SAMNAR was designed to operate in a distributed way, however it can be easily modified to work in a centralized way. The survival module holds five independent components. Four of them are related to resistance, recognition, recovery and adaptability, and the last one is the control component. The resistance component employs preventive mechanisms, such as firewall, access control, authentication and cryptography. The recognition component comprehends reactive mechanisms to identify malicious behaviors, such as IDSs, reputation systems, anti-malwares and anti-spammers.



ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 11, November 2014

The recovery component consists of mechanisms to enhance the attack tolerance of network essential services. The adaptation component complements the previous ones. It is responsible for adapting preventive, reactive and tolerant mechanisms, as well as local or network configurations. . The control component manages and coordinates all modules in the architecture. The communication module is responsible for cross-layer and inter-node communications. The inter-layer component offers the exchange of inter-layer information. The inter node component 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 pre-processing and environmental information components. The first one is exploited when gathered data need to be processed before sending to the survival module. The second component stores information gathered periodically about the network conditions, sending it to the survival module when required.

V. SURVIVAL PATH SELECTION SCHEME

Path selection scheme is a multi-criteria based scheme employing both conventional criteria and security criteria to point out the most survivable path.

A. 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. 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 components comprise fuzzification, fuzzy inference and path ranking. The path selection scheme employs fuzzy 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).

1. Fuzzification

Remaining energy is represented by the following linguistic terms: low, medium and high, in which the membership function of energy rate (E). 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:

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

Path length (L) denotes the number of intermediate hops between the source node and the destination node. Path length variable has three fuzzy sets: short, medium and long. 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. For cryptographic key length (K), two fuzzy sets are defined, short and long. If the secret key has 40 bits or less, it is considered short, and it is long with 128 bits or more The reputation (R) of a path i is the lowest node reputation value in the path. The reputation of the path i with n nodes is calculated as:

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

Path degree (D) represents tolerant defense lines, being defined by the minimum node degree among all n nodes participating in a path i. Path degree linguistic variable has three fuzzy sets: few, normal and many.

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

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

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

fuzzy set are combined by means of algebraic product operation. 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.

2. Fuzzy inference and path ranking

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, 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.

B. Collect and communication modules

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.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 11, November 2014

VI.EVALUATIONS OF THE PATH SELECTION SCHEME

It analyze the protocol-independent path selection scheme using Network Simulator (NS-2) version 2.30. Simulations were performed considering two types of multi-hop wireless ad hoc networks composed of n mobile or stationary nodes. Particularly, we have simulated an ad hoc network in which mobile nodes move into an area following a two-way random mobility, called CASE 1, and an urban mesh network employing a realistic node mobility and signal propagation, called CASE 2. The path selection scheme was instantiated on the routing protocol AOMDV (On-demand Multipath Distance Vector Routing in Ad Hoc Networks) .The AOMDV protocol was modified to provide security criteria values and to execute functionalities defined as data collection, fuzzy inference and path selection. It compare results produced by the AOMDV modification, called AOMDV-SL, with those yielded by AODV and AOMDV in the presence of attacks. It concentrate analyses on authorized nodes acting in a malicious or selfish fashion alone or in collusion. Attacks yielded by misbehaving (malicious or selfish) nodes, such as blackhole, grayhole, wormhole and sinkhole, cannot be prevented uniquely by authentication mechanisms. In blackhole attack, misbehaving nodes drop data packets, but they continue to participate in routing operations. Hence, whenever a misbehaving node is selected on a path, data will be lost on the path. Grayhole (selective forwarding) attack is a variant of blackhole attacks where misbehaving nodes will select which packet will be dropped. Those attacks select only packets of applications that are vulnerable to packet loss, such as real-time applications. Authentication techniques cannot prevent this attack. Wormhole results from colluding misbehaving nodes coordinating their actions. In wormhole attack, two colluding misbehaving nodes cooperate by tunnelling packets each other in order to create a shortcut in the network. This tunnel can be created by using a private communication channel, such as a pair of radios and directional antennas. In sinkhole attacks, a misbehaving node attracts surrounding nodes with unfaithful routing information, and then alters the data passing through it or performs other attacks, such as grayhole. In sinkhole attacks, a misbehaving node attracts surrounding nodes with unfaithful routing information, and then alters the data passing through it or performs other attacks, such as grayhole. Existing mechanisms against sinkhole are inefficient because of misbehaving nodes take off their correct participation in the routing process.

• **Misbehavior drop ratio (MDR)** - measures the proportion of data packets dropped due to attacks over the total of data packets dropped. For the sake of analyses, we have implemented mechanisms on NS-2 to log data packets maliciously dropped.

• **Packet delivery ratio (PDR)** - calculates the percentage of data packets delivered at the destination over the total amount of data packets sent by the source.

• **End-to-end delay of data packets (E2E delay)** – consists of propagation delays, queuing delays at interfaces, retransmissions delays at the MAC layer, as well as buffering delays during route discovery step.

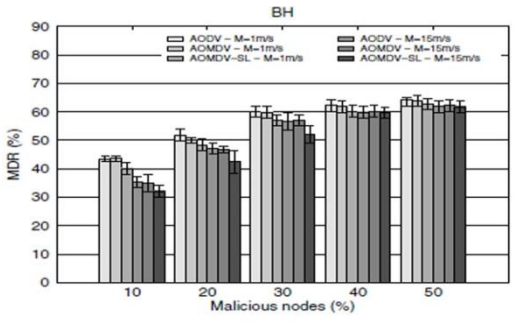
A. CASE 1: WIRELESS AD HOC NETWORKS

1. Simulation Settings

The IEEE 802.11 protocol operating with the distributed coordination function (DCF) is used as medium access control (MAC) protocol. The radio model presents similar characteristics to a commercial Lucent's WaveLAN radio interface with a nominal bit-rate of 2 Megabit per second (Mb/s) for the shared-media radio and nominal radio range (r) of 100 meters.This radio range was used to force a higher number of nodes in multi-hop paths. The mobility model applied is the random way-point model, in which node speeds are randomly chosen between zero meters per second (m/s) and a maximal speed (M) of 1 m/s and 15 m/s. The data traffic used in the simulations is CBR (Constant Bit Ratio) with 20 source nodes defined randomly. Each source generates data packets of 512 bytes and transmits them with a rate of 4 packets per second (pkt/s). The network area dimensions were fixed for all simulations in 1000 m by 300 m, and the total number of nodes n placed randomly in this area is of 50 nodes. In the beginning of each simulation, malicious nodes are chosen randomly from the total number of nodes. The total simulation time was 500 seconds and each plotted point is an average of 35 simulation.

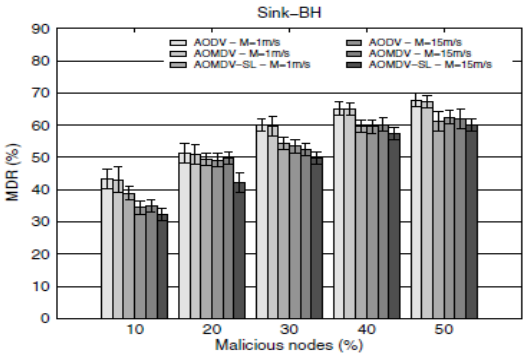
2. Simulation Results

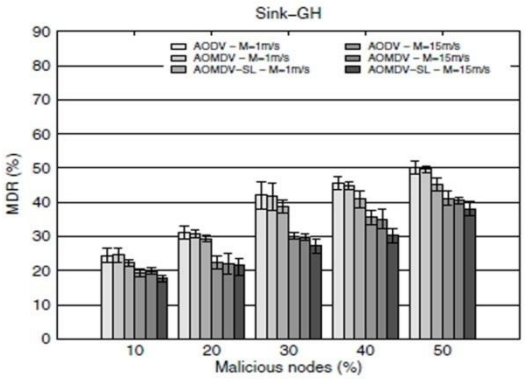
Here, compares the MDR resulted from AODV against sinkhole are inefficient because of misbehaving nodes take off their correct participation in the routing process. It examine the percentage of data packets dropped due to blackhole (BH), sinkhole combined with blackhole (Sink-BH) and sinkhole combined with grayhole (Sink-GH) attacks for all protocols.It observe that BH attacks result always in the highest ratio of packets dropped due to attacks (MDR) independent of the protocol. Considering this aspect, we verify that our scheme has improved the survivability of data packet, that is, it has reduced the MDR value in the presence of the three attacks. AOMDV-SL decreases the MDR compared to other protocols by 30% up to 50% of those produced by AODV or AOMDV in the presence of up to 20% of misbehaving nodes in the network



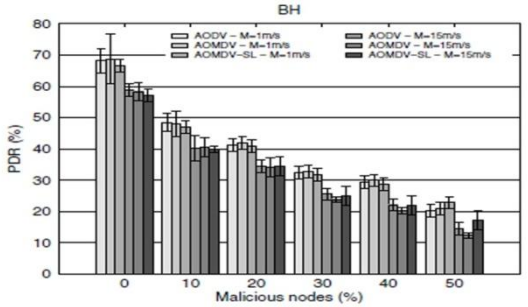
ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

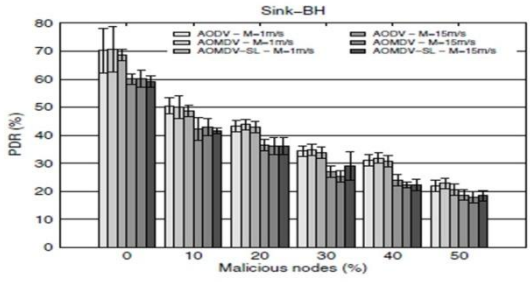
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 11, November 2014

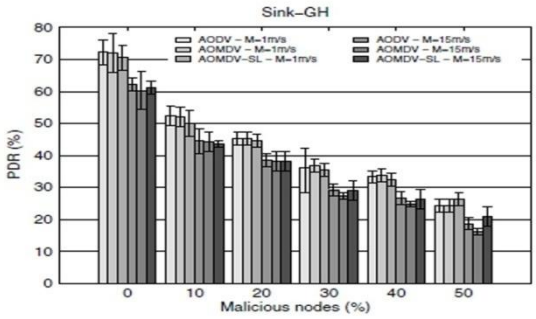




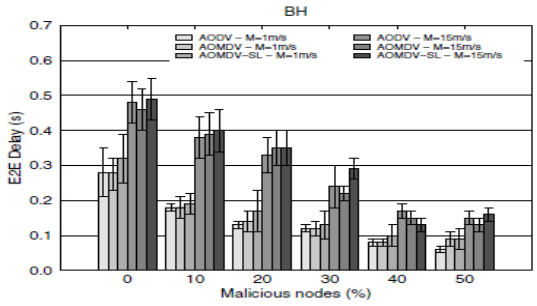
The results of PDR for all evaluated protocols considering *r* of 100 m. The PDR produced by AOMDV-SL varies about 5% up to 10% compared to PDR of AODV or AOMDV. However, the PDR of AOMDVSL is higher than those produced by AODV or AOMDV in lower percentage of misbehaving nodes, and this difference tends to be irrelevant for higher percentages

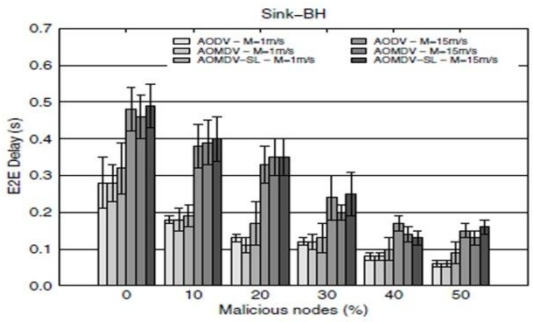


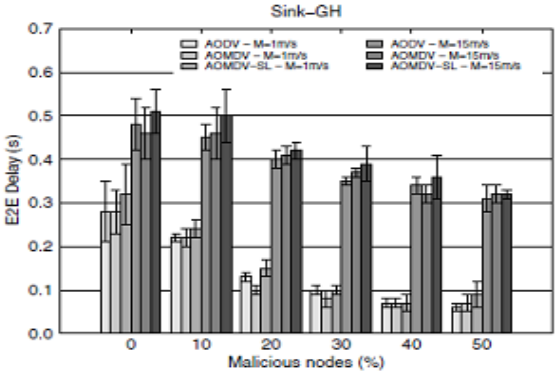




The difference between the latency produced by AOMDV-SL and by other protocols is independent of the attack and is almost constant for all misbehaving node percentages. When compared the AOMDV-SL latency with the latency of AODV and AOMDV on the same value of M, we verify that their latency is similar. Moreover, we observe that for all protocols the latency tends to decrease with the increase in the percentage of misbehaving nodes. The network latency under Sink-GH attack presented the worst case for all protocols when the percentage of misbehaving nodes is higher than 30%.







ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 11, November 2014

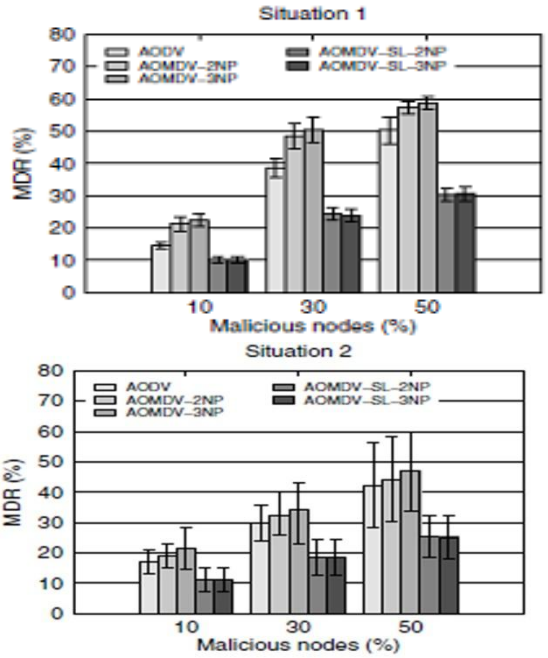
B. CASE 2: WIRELESS MESH NETWORKS

1. Simulation Settings

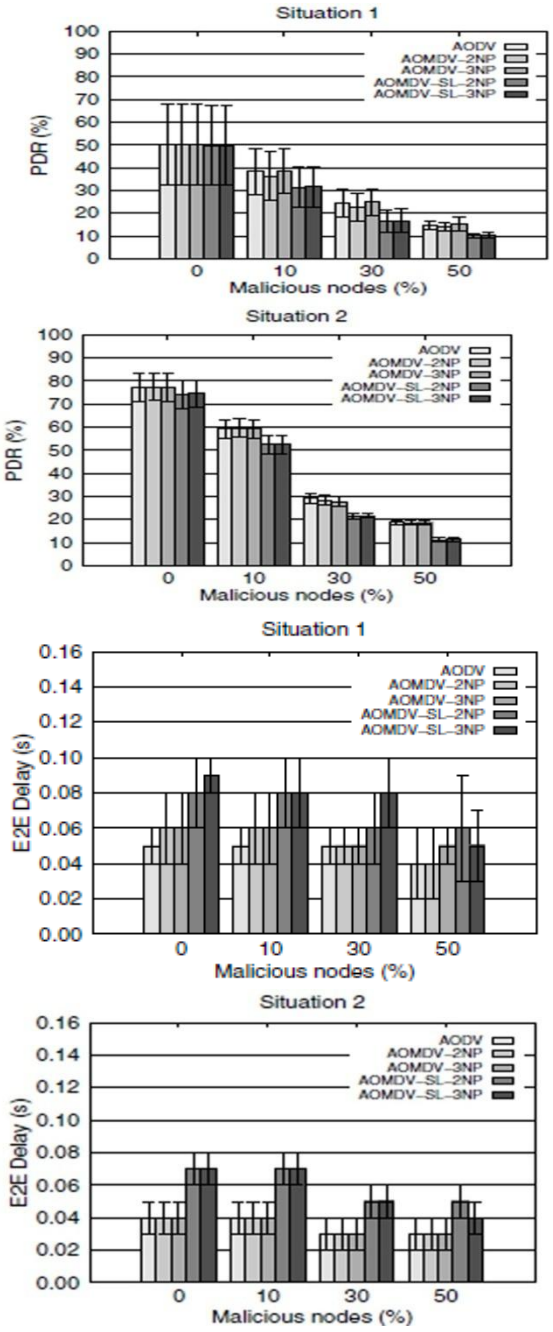
Nodes use the IEEE 802.11 distributed coordination function (DCF) as medium access control (MAC) protocol and IEEE 802.11b as radio model for communication with transmission power of 15 dBm and received card sensitivity of -93 dBm, receiving at 1 Mb/s. Each simulation was composed of 500 mobile nodes and 29 fixed infrastructure nodes distributed in an area of 500 meters by 500 meters. Evaluations investigate two situations. In Situation 1, changed the node mobility and signal propagation for each simulation in order to verify our scheme under different network movement patterns. Situation 2, observed the scheme under 35 independent simulations with different traffic behavior in each one, but with the same transmission rate (3 pkt/s).

2. Simulation results

It investigate the behavior of the misbehavior drop ratio (MDR) in Wireless Mesh Networks under Blackhole (BH) attacks. It observe that our scheme, AOMDV-SL,increases the survivability of data packets since it reduces the ratio of packets dropped due to attacks evaluated by the MDR. This can be observed when compared the MDR yielded by AOMDV-SL with AODV, AOMDV-2NP and AOMDV-3NP. The MDR of AOMDV-SL-2NP and AOMDV-SL-3NP reduces of 5% up to 28% the MDR found by the other protocols.



The PDR of AOMDV-SL, independently of the *NP* value, decreases compared to the PDR of AODV or AOMDV. The reduction on PDR using AOMDV-SL tends to increase with the rise in the misbehaving node percentages. However, it is always between 5% and 10%. The PDR for all evaluated protocols is lower in Situation 1, where different periods of the day are considered.



AOMDV-SL increases the network latency compared to AODV and AOMDV.

VII. CONCLUSION

This work presented a survivable management architecture for ad hoc and mesh networks called SAMNAR. Its goal lies in making these networks able to provide essential services even in face of attacks and intrusions. SAMNAR is based on a coordinated integration among the preventive, reactive and tolerant defense lines, being able to self-adapt to different network conditions. Based on SAMNAR, we designed a protocol-independent path selection scheme where a low-cost mechanism correlates security and conventional criteria to better choose survival paths and self-adapting to attacks and failures. We

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

evaluated survivability improvements and performance of our scheme by simulations where realistic node mobility and signal propagation were taken into account for WANETs. Results point out that our approach significantly decreases the impact of routing attacks with minimal performance loss.

REFERENCES

[1] Michele Nogueira , Helber , Aldri Santos, ,and Guy Pujolle, "A Security Management Architecture for Supporting Routing Services on WANETs" IEEE Trans. on Network and Service Management, Vol. 9, No. 2, June2012.
[2] W. Lou, W. Liu, and Y. Fang, "SPREAD: enhancing data confidentiality in mobile ad hoc networks," in Proc. 2004 IEEE INFOCOM, vol. 4, pp.2404–2413.
[3] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in Proc. 2000 ACM MobiCom,pp. 255–265.
[4] M. T. Refaei, V. Srivastava, L. DaSilva, and M. Eltoweissy, "A reputation-based mechanism for isolating selfish nodes in ad hoc networks," in Proc. 2005 MOBIQUITOUS, pp. 3–11.
[5] P. Papadimitratos and Z. J. Haas, "Secure data transmission in mobile ad hoc networks," in Proc. 2003 ACM WiSe, pp. 41–50.
[6] S. Paris, C. Nita-Rotaru, F. Martignon, and A. Capone, "Efw: a cross layer metric for reliable routing in wireless mesh networks with selfish participants," in Proc.2011 IEEE INFOCOM, pp. 576–580.
[7] M. Virendra, S. Upadhyaya, V. Kumar, and V. Anand, "SAWAN: a survivable architecture for wireless LANs," in Proc. 2005 IEEE IWIA,pp. 71–82.
[8] 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.
[9] P. Velloso, R. Laufer, D. de O Cunha, O. Duarte, and G. Pujolle, "Trust management in mobile ad hoc networks using a scalable maturity-based model," IEEE Trans. Network and Service Management, vol. 7, no. 3,pp. 172–185, 2010.
[10] Y. Yuan, S. Wong, S. Lu, and W. Arbaugh, "ROMER: resilient opportunistic mesh routing for wireless mesh networks," in 2005 IEEE WiMesh.

BIOGRAPHY

Arya.S.P completed her B.tech degree from Kerala University in 2011 and M.E degree from Anna University, Chennai in 2013. She is currently working as an Assistant Professor in Dept.CSE in a leading engineering college under Kerala University. Her area of interest includes Network Security, Computer networks, Mobile computing, Operating system and Data Structures.