IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 11, Issue 2, Ver. I (Mar-Apr .2016), PP 60-66
www.iosrjournals.org

A Study Of Wireless Mesh Networks Insider Attacks Of Selective Jamming Or Dropping

M. Sudhakar
Department Of ECE, CMR College of Engineering & Technology, India

Abstract: *Wireless mesh networks (WMNs) promise to increase high-speed wireless property on the far side what's attainable with the present WiFi-based infrastructure. However, their distinctive field options leave them notably prone to security threats. During this article, we tend to describe numerous varieties of refined attacks launched from adversaries with internal access to the WMN. We tend to any determine attainable detection and mitigation mechanisms.*

Keywords: *Security, misbehavior, wireless mesh networks, jamming, corporate executive attacks, packet dropping.*

I. Introduction

Wireless mesh networks (WMNs) still receive important interest as a attainable means that of providing seamless information property, particularly in urban situations [1]. Networks evolved from classic mobile impromptu networks, targeting long-range transmissions with stress on network outturn and property. WMN applications embrace stationary deployments (e.g., community networks, gradable detector networks) still as mobile ones (e.g., intelligent transportation systems, military science military networks).

WMNs follow a two-tier specification [2]. The primary tier consists of the tip users, additionally brought up as stations (STAs), directly connected to mesh nodes, brought up as Mesh Access Points. The second tier consists of a peer to peer network of the MAPs. Property within the second tier is aided by intermediate routers referred to as Mesh Points (MPs) that interconnect MAPs. The network of MAPs and MPs is commonly static and uses separate frequency bands to speak information and management data (MAPs area unit usually equipped with multiple transceivers). Finally, Mesh Gateways (MGs) give property to the wired infrastructure. Associate degree example of a WMN is shown in Fig. 1.

WMNs area unit invariably prone to “internal” and “external” attacks. An External attack take the varieties of random channel electronic jamming, packet replay, and packet fabrication, and area unit launched by “foreign” devices that area unit unaware of the network secrets (e.g., science credentials and pseudo-random spreading codes). They’re comparatively easier to counter through a mix of cryptography-based and strong communication techniques.

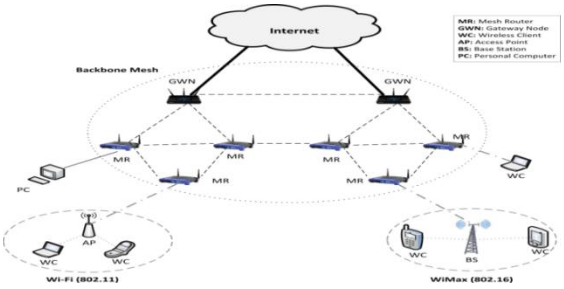

Fig. 1. WMN design

In distinction, internal attacks, that area unit launched from compromised nodes, area unit way more refined in nature. These attacks exploit data of network secrets and protocol linguistics to by selection and adaptively tar-get essential network functions. Attack property is achieved, as an example, by overhearing the primary few bits of a packet [3], or classification of transmissions supported protocol linguistics [4]. Internal attacks, henceforward brought up as corporate executive attacks, can't be slaked victimization solely proactive strategies that have confidence network secrets, as a result of the offender already has access to such secrets. They in addition need protocols with inbuilt security measures, through that the offender is detected and its selective nature is neutral.

Vulnerabilities of WMNs: whereas all kinds of wireless networks area unit at risk of corporate executive attacks, WMNs area unit notably prone to them, for variety of reasons. First, MPs and MAPs area unit comparatively low-cost devices with poor physical security, that makes them potential targets for node capture and compromise. Second, given their comparatively advanced hardware (e.g., multiple transceivers per MP and MAP), WMNs typically adopt a multi-channel style, with one or a lot of channels dedicated for control/broadcast functions. Such static style makes it easier for associate degree offender to by selection target control/broadcast data. Third, the reliance on multi-hop routes any accentuates the WMN vulnerability to compromised relays which might drop management messages, so as to enforce an explicit routing behavior (e.g., force packets to follow long or inconsistent routes).

In this paper, we tend to discuss numerous varieties of refined attacks in WMNs, during which associate degree corporate executive opponent showing intelligence exploits data of leaked science secrets and of protocol linguistics to attack essential net-work functions like channel access, routing, and end-to-end reliable information delivery. we tend to focus our attention on corporate executive attacks that take the shape of electronic jamming and/or dropping of high value packets in any given layer or else combination of layers. Whereas electronic jamming aims at preventing reception whereas the packet is in transmission, selective dropping is applied post-reception. Besides describing such attacks, we tend to additionally high-light attainable detection and mitigation mechanisms.

II. Selective Jamming Attacks

The open nature of the wireless medium leaves it prone to jam attacks. jam in wireless networks has been primarily analyzed underneath associate degree external adversarial model, as a severe style of denial of service (DoS) against the PHY layer. Existing anti-jamming ways use some style of unfold spectrum (SS) communication, within which the signal is unfold across an outsized information measure in step with a pseudo-noise (PN) code. However, SS will defend wireless communications solely to the extent that the PN codes stay secret. Insiders with information of the usually shared PN codes will still launch jam attacks. mistreatment their information of the protocols specifics, they will by selection target explicit channels/layers/protocols/packets. we tend to describe 2 kinds of electronic jamming attacks against WMNs, that use channel and knowledge property.

A. Channel-Selective jam

In a typical WMN, one or additional channels square measure reserved for broadcasting management data. These channels, observed as management channels, facilitate operations like network discovery, time synchronization, coordination of shared medium access, routing path discovery et al, while not meddlesome with the communications of STAs with MAPs. associate degree antagonist United Nations agency by selection targets the management channels will with efficiency launch a DoS attack with a reasonably restricted quantity of resources (control traffic is low-rate compared to knowledge traffic). To launch a channel-selective jam attack, the antagonist should bear in mind of the situation of the targeted channel, whether or not outlined by a separate band, time slot, or PN code. Note that management channels square measure inherently broadcast and thence, each meant receiver should bear in mind of the secrets wont to defend the transmission of management packets. The compromise of one receiver, be it a MAP or associate degree MP, reveals those secrets to the antagonist.

Example: we tend to illustrate the impact of channel-selective jam on CSMA/CA-based medium access management (MAC) protocols for multi-channel WMNs. A multi-channel mac (MMAC) protocol is used to coordinate access of multiple nodes residing within the same collision domain to the common set of channels. a category of MMAC protocols planned for unintended networks like WMNs follows a split-phase style (e.g., [5]). during this style, time is split into alternating management and knowledge transmission phases. throughout the management part, each node converges to a default channel to barter the channel assignment. within the knowledge transmission part, devices switch to the in agreement on channels to perform knowledge transmissions. The alternating phases of a split-phase MMAC square measure shown in Fig. 2.

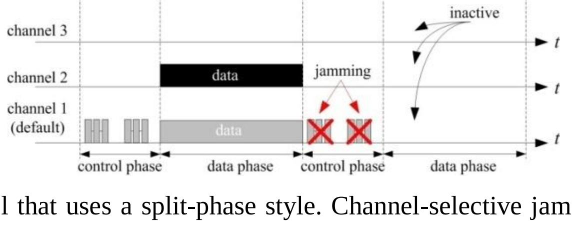

Fig. 2. A MMAC protocol that uses a split-phase style. Channel-selective jam of the default channel throughout the management part prevents the utilization of all channels throughout the info transmission part.

By using a channel-selective strategy, an enclosed antagonist will jam solely the default channel and solely throughout the management part. Any node that's unable to access the default channel throughout the management part should defer the channel negotiation method to following management part, therefore remaining inactive throughout the subsequent knowledge transmission part. This attack is illustrated in Fig. 2. Note that the impact of this channel-selective jam attack propagates to all or any frequency bands at an occasional energy overhead, since solely one channel is targeted and just for a fraction of your time.

B. Countering Channel-Selective Attacks

Several anti-jamming ways are planned to deal with channel-selective attacks from corporate executive nodes. All ways trade communication potency for stronger resilience to jam. we tend to provides a transient description of such anti-jamming approaches.

Replication of management data: associate degree intuitive approach to counter channel-selective jam is to repeat management information on multiple broadcast channels [6]. during this case, associate degree corporate executive with restricted hardware resources cannot jam all broadcasts at the same time. Moreover, if every node has solely partial information of the locations of the published channels, associate degree corporate executive will target solely the set of channels familiar to him. attributable to the restricted range of obtainable channels, this theme provides protection against alittle range of colluding attackers.

Assignment of distinctive PN codes: an alternate technique for neutralizing channel-selective attacks is to dynamically vary the situation of the published channel, supported the physical location of the communication nodes [7]. the most motivation for this design is that any broadcast is inherently confined to the communication vary of the broadcaster. Hence, for broadcasts meant for receivers in several collision domains, there's no explicit advantage in mistreatment constant broadcast channel, apart from the look simplicity. The assignment totally different broadcast channels to different network regions results in associate degree inherent partitioning of the network into clusters. Data concerning the situation of the management channel in one cluster can't be exploited at another. Moreover, broadcast communication will be repaired regionally ought to a transmitter seem, while not the necessity for re-establishing a world broadcast channel. To shield the management channel among every cluster, following cluster formation, one mesh node is electoral because the cluster head (CH). The CH assigns its cluster members distinctive PN hopping sequences that have vital over-lap. The common locations among these PN sequences implement a broadcast channel. If associate degree corporate executive uses his PN sequence to jam this broadcast channel, it becomes unambiguously recognizable by the CH. Once known, the CH updates all nodes of the cluster with new PN sequences, apart from the known offender. the thought of assignment distinctive PN codes to numerous nodes within the network was additionally exploited in [8]. during this work, nodes of a cluster square measure depicted by the leaves of a binary tree. every node of the tree is allotted a novel key, similar to a seed for the generation of a novel PN code. each node is aware of all the keys on the trail from the corresponding leaf to the foundation. within the absence of jam, the PN code familiar to all or any receivers (generated by the foundation key) is employed. If jam is detected, sending nodes switch to a PN code familiar solely to a set of nodes. The compromised node is unambiguously known in a very range of steps that's power to the quantity of nodes among the cluster.

Elimination of secrets: Selective corporate executive jam attacks will be countered by avoiding secrets within the 1st place. Within the style planned in [9], a transmitter at random selects a PN code from a public codebook. To recover a transmitted packet, receivers should record the transmitted signal and try decipherment it mistreatment each PN code within the codebook. As a result of the PN code wont to unfold every packet isn't familiar a priori, an enclosed antagonist will solely conceive to guess it, with a restricted likelihood of success. Special care has to incline to the synchronization between the communication parties (knowing the PN code is important for locating and “locking onto” the transmitted signal).

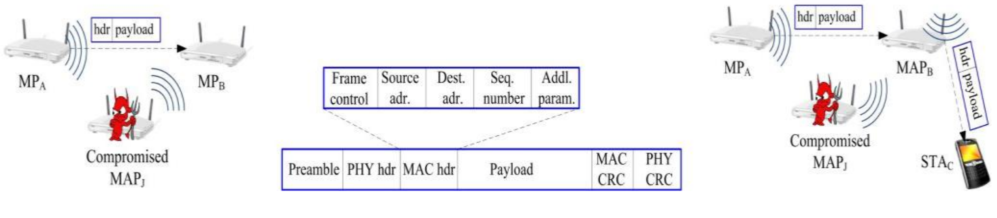

Fig. 3. (a) A data-selective jam attack, (b) generic packet format, (c) logical thinking of a RREP transmission on link MAPB-STAC supported the RREP transmission on link MPA-MAPB.

C. Data-Selective jam

To more improve the energy potency of electronic jamming and cut back the chance of detection, an enclosed offender will exercise a larger degree of property by targeting specific packets of high importance. a technique of launching a data-selective jam attack, is by classifying packets before their transmission is completed. associate degree example of this attack is shown in Fig. 3(a). MPA transmits a packet to MPB. within offender MAPJ classifies the transmitted packet once overhearing its 1st few bytes. MAPJ then interferes with the reception of the remainder of the packet at MPB:

Referring to the generic packet format in Fig. 3(b), a packet will be classified supported the headers of varied layers. as an example, the MAC header usually contains data regarding following hop and also the packet kind. The protocol header reveals the end-to-end supply and destination nodes, the transport-layer packet kind (SYN, ACK, DATA, etc.), and different protocol parameters.

Another technique for packet classification is to anticipate a transmission supported protocol linguistics. As associate degree example, take into account the routing perform in WNMs, delineate within the IEEE 802.11s normal [2]. Routing is performed at the MAC layer in step with the Hybrid Wireless Mesh Protocol (HWMP). The latter could be a combination of tree-based routing, and on-demand routing supported AODV. Tree-based routing provides fastened path routes from the mesh nodes to the MGs. On demand routing is used to get routes to mobile STAs United Nations agency escort multiple MAPs attributable to their quality. take into account the route discovery method delineate in Fig. 3(c). MPA transmits a route reply (RREP) to MAPB, that is overheard by MAPJ . MAPJ will conjecture that MAPB can forward the RREP to STAC, and hence, jam this RREP whereas it's in transit to STAC.

Packet classification may be achieved by observant implicit packet identifiers like packet length, or precise protocol temporal order data [4]. as an example, management packets square measure typically a lot of smaller than knowledge packets. The packet length of associate degree eminent transmission will be inferred by decipherment the network allocation vector field (NAV) of request-to-send (RTS) and clear-to-send (CTS) messages, used for reserving the wireless medium.

D. Countering Data-Selective jam Attacks

An intuitive resolution for preventing packet classification is to write in code transmitted packets with a secret key. during this case, the whole packet, as well as its headers, must be encrypted. whereas a shared key suffices to shield point-to-point-communications, for broadcast packets, this key should be shared by all meant receivers. Thus, this secret's additionally familiar to an enclosed transmitter. In biradial coding schemes supported block coding, reception of 1 cipher text block is sufficient to get the corresponding plaintext block, if the cryptography secret's familiar. Hence, coding alone doesn't forestall insiders from classifying broadcasted packets.

To prevent classification, a packet should stay hidden till it's transmitted in its completeness. One doable means for quickly concealing the transmitted packet is to use commitment schemes. in a very commitment theme, the sending node hides the packet by broadcasting a committed version of it. The contents of the packet can't be inferred by receiving the commitment (hiding property). once the transmission is completed, the node releases a de-commitment price, that reveals the initial packet. The commitment theme should be rigorously designed to forestall the classification of the initial packet supported the partial unharnessed of the de-commitment price. Another approach is to use public concealing trans-formations that don't accept secrets. associate degree example of them is all-or-nothing transformations (AONTs), that were originally planned to cut down brute force search attacks against coding schemes. associate degree AONT is a in public familiar and fully invertible pre-processing step for a plaintext, before it's passed to associate degree coding rule. The process property of associate degree AONT is that the whole output of the transformation should be familiar before any a part of the input will be computed. In our context, associate degree AONT prevents packet classification once the AONT of a packet is transmitted over the wireless medium.

III. Selective Dropping Attacks

If jam isn't winning attributable to anti-jamming measures, associate business executive will by selection drop packets post reception. Once a packet has been received, the compromised node will examine the packet headers, classify the packet, and choose whether or not to forward it or not. Such associate action is commonly termed as wrongful conduct [10]–[13]. Post-reception dropping is a smaller amount versatile than jam as a result of the resister is restricted to dropping solely the packets routed through it. nevertheless, the impact on the WMN performance will be important.

Examples: think about a compromised MP targeting the routing practicality in WMNs. By selection dropping route request and route reply packets utilized by the routing protocol, as outlined within the of the 802.11s customary [2], the compromised MP will stop the invention of any route that passes through it, delay the route discovery method, and force different, probably inefficient ways. Instead, the compromised MP will enable the institution of a route via itself; however throttle the speed of the end-to-end affiliation at the transport layer. This attack will be actualized by selective dropping of vital management packets that regulate the end-to-end transmission rate and effective outturn. As an example, the dropping of accumulative transmission control protocol acknowledgments ends up in the end-to-end retransmission of the complete batch of unfinished knowledge packets (see Fig. 4). Additionally, packet loss is taken as congestion, leading to the asphyxiation of the sender's transmission rate.

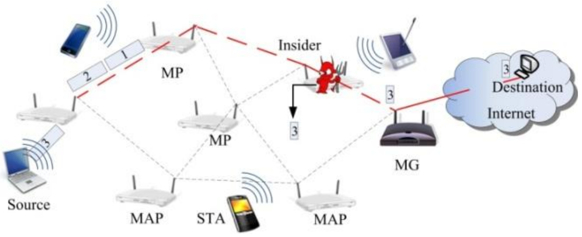

Fig. 4. Associate business executive by selection drops accumulative transmission control protocol acknowledgments and forces end-to-end knowledge retransmissions.

In another selective strategy referred to as the Jellyfish attack, a compromised mesh node that sporadically drops a tiny low fraction of consecutive packets will effectively reduce the outturn of a transmission control protocol flow to close zero [14]. This attack will be achieved even by causation random delays to transmission control protocol packets, while not dropping them, whereas remaining protocol compliant [14]. Similar selective dropping attacks will be made for alternative network functions like the association/de-association of STAs, and topology management, to call a couple of.

A. Mitigation of Selective Dropping

Selective dropping attacks will be lessened by using fault-tolerant mechanisms at varied layers of the protocol stack. At the routing layer, multi-path routing provides strong multi-hop communication within the presence of network faults, by utilizing over one path from a supply to a destination. Tree-based routing in HWMP already provisions for back-up ways to the MG [2]. At the transport layer, variants of the standardized transmission control protocol are specifically developed for coping with the imperfections of the wireless medium [15]. These protocols differentiate between congestion and wireless transmission losses. A selective dropper will continually attribute his losses to congestion, so as to avoid detection as a malicious node. during this case, identification mechanisms using long-run statistics, will accurately pinpoint selective droppers.

B. Identification of Selective Droppers

Current strategies for police investigation wrongful conduct in self-organizing systems like WMNs, will be classified into name systems [12], credit-based systems [13], and acknowledgment systems [10].

Reputation Systems: name systems establish misbehaving nodes supported per-node name metrics, computed supported interactions of every node with its peers. These systems usually incorporate 2 vital operations: (a) the gathering of correct observations of nodes' behavior and, (b) the computation of the name metric.

Behavioral data is collected supported first-hand observations provided by neighboring nodes and second-hand data provided by alternative interacting peers [12]. First-hand observations are collected by observation nodes that operate in promiscuous mode so as to verify the proper forwarding of transmitted packets. Overhearing becomes problematic within the case of multi-channel WMNs, as a result of MPs and MAPs are regular to speak in parallel over orthogonal frequency bands, and hence, they could not be obtainable to observe the behavior of alternative nodes. Many schemes are planned for managing second-hand data. A node might flood warnings to the complete network, if it detects a misbehaving node. instead, data will be provided on-demand, when an invitation from a selected node has been received. within the latter situation, flooding of the request is important to get nodes that possess second-hand data. each strategies consume extended information measure resources attributable to the underlying flooding operations for the dissemination and assortment of second-hand data.

Robust computation of name metrics is equally vital for the identification of packet droppers. Easy mixture metrics are shown to be liable to false accusations from colluding malicious nodes, and suddenly dynamical behavioural patterns. As an example, a misbehaving node will exhibit an extended history of excellent behavior so as to make a high name metric, before it starts to act. Such instances are dealt by distribution larger weights to recent behavioural observations and/or adopting additive increase-multiplicative decrease kind of algorithms for change the name metrics [12].

A vital challenge for any metric computation formula is that the selective nature of packet droppers. once a really tiny fraction of packets is born, metrics that don't take under consideration the packet kind are certain to have high rates of misdetection. Dropping property will be detected with the employment of storage-efficient reports (e.g., supported Bloom filters) of the per-packet behavior of nodes [11]. supported these reports, it's doable to conduct multiple tests to spot malicious selective dropping patterns. These patterns are possible to possess some settled structure compared to packet losses attributable to congestion or poor channel quality.

ACK-based systems: ACK-based schemes take issue from overhearing techniques within the methodology of aggregation first-hand behavioural observations. Downstream nodes (more than one hop away) are to blame for acknowledging the reception of messages to nodes many hops upstream [10]. These systems are appropriate for observation the devoted relay of unicast traffic, at the expense of communication overhead for relaying a further set of ACKs. However, ACK-based schemes can't be accustomed establish insiders that by selection drop broadcast packets. Such packets stay, in general, unacknowledged in wireless networks, to avoid associate ACK implosion scenario. Moreover, a tiny low set of colluding nodes will still give authentic ACKs to upstream nodes whereas dropping packets.

Credit-based systems: Credit-based systems alleviate self-serving behavior by incentivising nodes to forward packets [13]. Nodes that relay traffic receive credit reciprocally, which may be later spent to forward their own traffic. However, within the context of WNMs, MPs don't generate any traffic of their own, however act as dedicated relays. Hence, compromised MPs don't have any incentive for aggregation credit. Moreover, within the case of selective dropping attacks, misbehaving nodes will still collect sufficient credit by forwarding packets of low importance, whereas dropping a couple of packets of "high price." additionally, the credit collected by a selected node depends on the topology of the network. A extremely connected node is predicted to gather additional credit attributable to the augmented volumes of traffic routed through it. associate resister compromising such a node is probably going able to implement a selective dropping strategy while not running out of credit. Finally, credit-based systems lack a mechanism for characteristic the misbehaving node(s), permitting them to stay inside the network indefinitely.

IV. Discussion And Conclusions

WMNs are at risk of varied external and internal security threats. Whereas most external attacks may be mitigated with a mixture of crypto graphical mechanisms and strong communication techniques, internal attacks are abundant tougher to counter as a result of the antagonist is tuned in to the network secrets and its protocols. Jamming-resistant broadcast communications within the presence of within jammers remains a difficult drawback. Current solutions arrange to eliminate the employment of common secrets for safeguarding broadcast communications. Such secrets may be simply exposed within the event of node compromise. However, the heightened level of security comes at the expense of performance, as a result of broadcasted messages have to be compelled to be transmitted multiple times and on multiple frequency bands to ensure strong reception.

Moreover, notwithstanding packet reception of crucial messages is ensured, within adversaries are in complete management of the traffic routed through them. An oversized body of literature addresses the matter of misbehavior within the style of packet dropping by developing name systems, credit-based systems, and communication-intensive acknowledgment schemes. Despite the relative wealth of literature on this drawback, vital challenges are nevertheless to be addressed. Most existing strategies assume a ceaselessly active antagonist that consistently drops packets. These adversaries are detected by mixture activity metrics like per-packet name and credit. However, these metrics cannot discover attacks of selective nature, wherever solely a little fraction of "high value" packets is targeted. What is more, once the antagonist drops solely some packets, his behavior may be indistinguishable from dropping patterns thanks to congestion or poor wireless conditions. Any challenges embrace economical activity watching mechanisms not wishing on continuous overhearing and economical maintenance and dissemination of name metrics.

References

[1]. I.F. Akyildiz, X. Wang, and W. Wang. Wireless mesh networks: a survey. Computer Networks, 47(4):445–487, 2005.

[2]. IEEE P802.11s/D1.01 standard. At https: //mentor.ieee.org/802.11/dcn/07/11-07-0335-00-000s-tgs-redline-between-draft-d1-00-and-d1-01.pdf, 2007.

[3]. Alejandro Proano and Loukas Lazos. Selective jamming attacks in wireless networks. In Proceedings of the IEEE International Conference on Communications (ICC), 2010.

[4]. T.X. Brown, J.E. James, and A. Sethi. Jamming and sensing of encrypted wireless ad hoc networks. In Proceedings of the 7th ACM International Symposium on Mobile ad hoc networking and computing, 2006.

[5]. J. So and N.H. Vaidya. Multi-channel MAC for ad hoc net-works: handling multi-channel hidden terminals using a single transceiver. In Proceedings of the ACM MobiHoc Conference, pages 222–233, 2004.

[6]. P. Tague, M. Li, and R. Poovendran. Probabilistic mitigation of control channel jamming via random key distribution. In Proceedings of the International Symposium in Personal, Indoor and Mobile Radio Communications (PIMRC), pages 1–5, 2007.

[7]. L. Lazos, S. Liu, and M. Krunz. Mitigating control-channel jamming attacks in multi-channel ad hoc networks. In Pro-ceedings of the Second ACM Conference on Wireless Network Security (WiSec), pages 169–180, 2009.

[8]. Jerry Chiang and Yih-Chun Hu. Cross-layer jamming detection and mitigation in wireless broadcast networks. In Proceedings of the ACM MobiCom Conference, pages 346–349, 2007.

[9]. Christina Popper,´ Mario Strasser, and Srdjan Capkun. Jamming-resistant broadcast communication without shared keys. In Proceedings of the USENIX Security Symposium, 2009.

[10]. K. Liu, J. Deng, P.K. Varshney, and K. Balakrishnan. An acknowledgment-based approach for the detection of routing misbehavior in MANETs. IEEE Transactions on Mobile Computing, 6(5):536–550, 2007.

[11]. W. Kozma and L. Lazos. Dealing with liars: Misbehavior identification via Renyi´-Ulam games. In Security and Privacy in Communication Networks, pages 207–227, 2009.

[12]. Han Yu, Zhiqi Shen, Chunyan Miao, C. Leung, and D. Niyato. A survey of trust and reputation management systems in wire-less communications. Proceedings of the IEEE, 98(10):1755 –1772, 2010.

[13]. Y. Zhang, W. Lou, W. Liu, and Y. Fang. A secure incentive protocol for mobile ad hoc networks. Wireless Networks, 13(5):569–582, 2007.

[14]. Imad Aad, Jean-Pierre Hubaux, and Edward W. Knightly. Im-pact of denial of service attacks on ad hoc networks. IEEE/ACM Transactions on Networking, 16(4):791–802, 2008.

[15]. J. Liu and S. Singh. ATCP: TCP for mobile ad hoc net-works. IEEE Journal on Selected Areas in Communications, 19(7):1300–1315, 2002.

Author Biography

Dr. M. Sudhakar: Graduated from JNTU College of Engineering, Hyderabad in 1979, with specialization in ECE. He completed his M.Tech from Indian Institute of Technology Madras in 1986 with the specialization in Instrumentation, Control & Guidance. Obtained doctoral degree from Annamalai University. Successfully headed R&D Project assigned by IAF on "Mathematical Modelling & Simulation of Aero Engine Control System‟ at Aeronautical Development Establishment, Bangalore and Gas Turbine Research Establishment, Bangalore. He is presently working as a Professor in the department of ECE and Vice Principal at CMR College of Engineering & Technology, Hyderabad.