International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

A Study of Mitigating Misrouting Through Multi-Radio Multi-Channel MAC (M2-MAC) Protocol For Wireless Mesh Networks

Boopathy P
Curriculum Developer, PANACEA Research Midway, Chennai, Tamil Nadu, India

ABSTRACT

Much of the current research in wireless mesh networks has focused on protocols, algorithms and authentication schemes for protecting the data during data transmission. The wireless mesh network communication has become an explicating and important technology in recent years because of the rapid proliferation of wireless devices. WMN are highly vulnerable to attacks due to the open medium, dynamically changing network topology. This paper proposes and evaluates strategies to build reliable and secure communication in multi –radio multi-channel mesh networks using M2-MAC protocol. Therefore, we analyse mitigating misrouting in wireless multi- radio multi-channel using M2-MAC protocol and extensively show that our scheme provides very good enhancements in a variety of scenarios.

Keywords: M2-MAC protocol, Wireless Mesh Networks, Stealthy Attack, Routing Misbehaviour.

I. INTRODUCTION

As various wireless networks evolve into the next generation to provide better services, a key technology, wireless mesh networks (WMNs), has emerged recently. In WMNs, nodes are comprised of mesh routers and mesh clients. Each node operates not only as a host but also as a router, forwarding packets on behalf of other nodes that may not be within direct wireless transmission range of their destinations.

A WMN is dynamically self-organized and self-configured, with the nodes in the network automatically establishing and maintaining mesh connectivity among themselves (creating, in effect, an ad hoc network). This feature brings many advantages to WMNs such as low up-front cost, easy network maintenance, robustness, and reliable service coverage.

Security Attacks in Wireless Mess Networks

Security means protecting the privacy (confidentiality), availability, integrity and non-repudiation. Security implies the identification of potential attacks from unauthorized access, uses, modification or destruction. A *security attack* is any action that compromises the security of information in an unauthorized way. The attack may alter, release, or denial of data [8][9][10]. The attacks on the MANETs can be broadly classified into two categories: passive and active attacks. Both passive and active attacks can be made on any layer of the network protocol stack [3].

Stealth Attacks - Stealth attacks are classified into two classes. The first class of attacks attempts to perform traffic analysis on filtered traffic to and from victim nodes. The second class partitions the network and reduces good put by disconnecting victim nodes in several ways. The methods are referred to as *stealth* attacks since they minimize the cost of launching the attacks [13].

Security is always a critical step to deploy and manage WMNs. Similar to mobile ad hoc networks; WMNs still lack efficient and scalable security solutions because their security is easier to be compromised due to [11]: vulnerability of channels and nodes in the shared wireless medium, absence of infrastructure, and dynamic change of network topology. The attacks may advertise routing updates in wireless security [3] and [2] for DSR and AODV, respectively.

Another type of attacks is packet forwarding, i.e., the attacker may not change routing tables, but the packets on the routing path may be lead to a different destination that is not consistent with the routing protocol. Moreover, the attacker may sneak into the network, and impersonate a legitimate node and does not follow the required specifications of a routing protocol [6]. Some malicious nodes may create wormhole and shortcut the normal flows among legitimate nodes [7]. Same types of attacks as in routing protocols may also occur in MAC protocols.

Attackers may sneak into the network by misusing the cryptographic primitives [4]. In a cryptographic protocol, the exchange of information among users occurs frequently. The users employ a fair exchange protocol, which depends on a trusted third party. However, this trusted party is not available in WMNs due to lack of infrastructure. Thus, another exchange scheme, called rational exchange, must be used. Rational exchange ensures that a misbehaving party cannot gain anything from misbehaviour, and thus, will not have any incentives to misbehave [5].

To prevent possible security attacks, MANETs need secure routing protocols. There exist various secure routing protocols, such as SAR, ARAN, SAODV, SRP, ARIADNE, SEAD, SMT, SLSP, CONFIDANT, etc. in the literature and widely evaluated for efficient routing of packets [3][4]. However, these protocols are either too expensive or have unrealistic requirements. They consume many resources, and delay or even prevent successful exchanges of routing information. Security extensions for existing routing protocols do not contain important performance optimizations.

In this paper, we make the following contributions:

- We provide a primitive that prevent a malicious node and show how the protocol needs to be configured to achieve required detection as well as detecting several different attacks.
- We develop a protocol called M2-MAC that can detect and diagnose misrouting attacks in mesh networks.
- We provide a technique in M2-MAC to isolate malicious nodes from the network, thereby removing their ability to cause future damage.
- We analyze the detection latency and overhead of our solution and provide extensive simulations to study the efficiency of our approach.

II. RELATED WORK

In the last few years, researchers have been actively exploring many mechanisms to ensure the security of control and data traffic in wireless networks. These mechanisms can be broadly categorized into following classes- cryptographic building blocks used as support for key management, authentication and integrity services, protocols that relay on path diversity, protocols that overhear neighbour communication, protocols that use specialized hardware and protocols that require explicit acknowledgement are also used as building blocks for protocols of the other classes.[14].

The four modes of the stealthy packet dropping attack. [15]. we distinguish between an external malicious node, which does not possess the cryptographic keys in the network, and internal compromised nodes, which do and are created by compromising an erstwhile legitimate node. Consider a scenario in which a node called S is forwarding a packet to a compromised node called *M*. *M* is supposed to relay the packet to the next-hop node *D*. The first form of the attack is called *packet misrouting*. In this mode, M relays the packet to the wrong next –hop neighbour.
Baseline local monitoring [BLM] is a collaborative Strategy where a node monitors the control traffic going in and out of its neighbours.

The rest of the paper is organized as follows section 3 talks about the description of stealthy dropping attack. Section 4 describes the M2-MAC protocol for wireless mesh networks. Section 5 explains the Mitigation Misrouting Packet Drop over (M2-MAC) protocol. Section 6 concludes the paper.

III. STEALTHY DROPPING ATTACK

In all the modes of stealthy packet dropping, a malicious intermediate node achieves the same objective as if it were dropping a packet. However, none of the guard nodes using BLM becomes any wiser due to the action. In addition, a legitimate node is accused of packet dropping. Next, we describe the four attack types for stealthy dropping.

3.1 Drop through Misrouting:

In the misrouting attack, a malicious node relays the packet to the wrong next hop, which results in a packet

drop. Note that, in BLM [16], a node that receives a packet to relay without being in the route to the destination either drops the packet or sends a one-hop broadcast that it has no route to the destination. The authors in [16] argue that the latter case would be more expensive and dangerous since it gives malicious nodes valid excuses to drop packets. Therefore, they go with the first choice, even though it may result in some false accusations.

Consider the example scenario in Figure No 1. Node A sends a packet to the malicious node M to be relayed to node B. Node M simply relays the packet to node E that is not in the route to the final destination of the packet. Node E drops the packet.

The result is twofold: 1) node M successfully drops the packet without being detected since all the guards of M over A --> M (regions I and II) have been satisfied by the transmission of M --> E and 2) legitimate node E will be wrongly accused by its guards over M -> E (regions II and III) as maliciously dropping the packet.

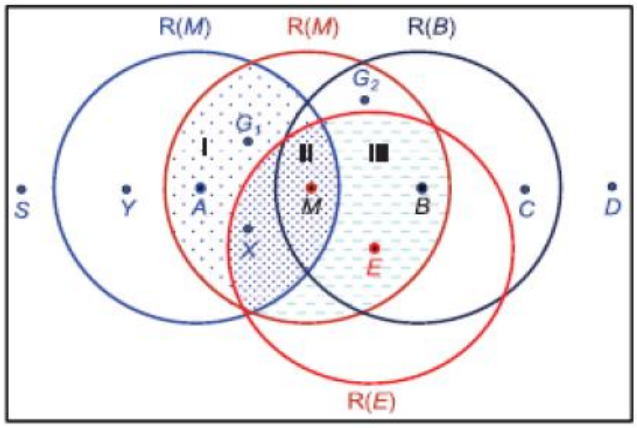

Figure 1: Misrouting state

IV. DESCRIPTION OF M2-MAC PROTOCOL

4.1 Overview of MAC protocol

If more than one channel is available and the network size is large, it is logical to allocate the stations to operate in different channels in order to improve system throughput. This is acceptable if communication is confined to the stations in the same channel. Otherwise, special equipment will be needed to bridge the stations in different channels to allow cross-channel communication. However, in ad hoc networks, such equipment is usually not available.

Therefore, there are two potential problems when single-channel MAC is used in multi-channel environment: connectivity and load balancing. The lack of connectivity limits networking power while the unbalanced load on different channels results in lower overall system throughput.

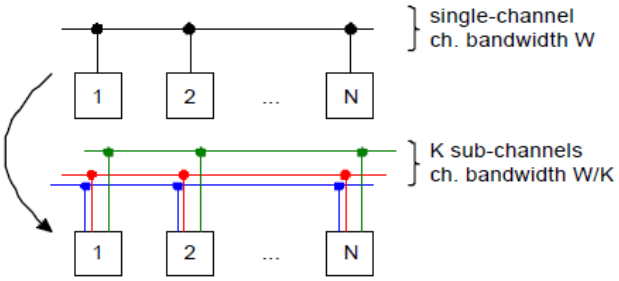

Figure 2a: Multi channel system by dividing a fat channel into multiple thin channels

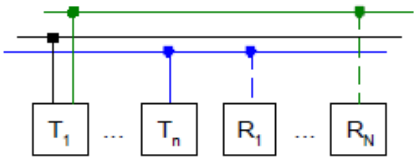

Figure 2b: Transmitter oriented multichannel system

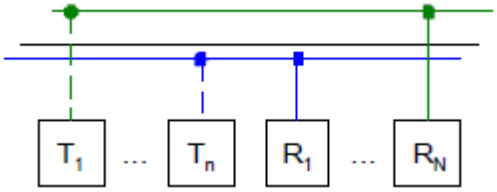

Figure 2c: Receiver oriented multichannel system

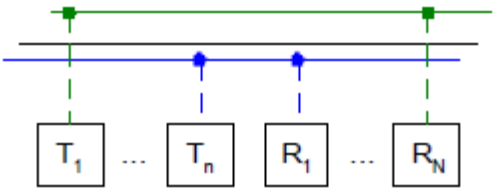

Figure 2d: Dynamic assigned multichannel system

Multi-channel MAC protocol different from single channel protocol, which allows to access more than one channel. Different forms of multichannel have been proposed in the literary. The authors in [18] and [19] show that by breaking down a channel into multiple sub-channels, the system performance will be improved for CSMA type protocol due to the reduction of normalized delay and probability of collision. The

model of this approach is shown in Figure No 2a**.** It requires each station to monitor all the channels at all time. IEEE 802.11a [17] adapts a similar model by using multiple OFDM channels to achieve total bit rate up to 54 mbps.

Another method on using multichannel is to have transmitter-receiver pair switches to the same channel when communication is required. The channel allocation mechanism can be either transmitter-oriented, receiver-oriented, or dynamically assigned [20] as shown in Figure No 2b, Figure No 2c and Figure No 2d. The transmitter-oriented mechanism has been used in point-to-multipoint systems such as satellite TV and radio broadcasting. Cellular phone system is an example of using dynamic assignment in which different calls are assigned different channels for the mobile-and-base connection during the period of a call.

4.2 M2-MAC Protocol Structure

M2-MAC is a secure routing protocol for mitigating misrouting over an insecure multi-radio multi-channel wireless mesh networks.
The M2-MAC protocol provides node authentication, confidentiality, and integrity, M2-MAC utilizes two types of messages, control messages and data messages. Control message specifies and allocate all channels as common control channels for coordinate the communication pair nodes. Data messages are used to dynamic channel allocation for data transmission by based on node ID, available channel for data transmission and the radio's channel utilization on the node.
M2-MAC contain all the essential information required for transfer the data in secure manner in network services, such as (header authentication, payload encapsulation , identity of hops and database of verification table), Which is defines, the header authentication carries the identity of all the nodes in the route. These formats provide a consistent framework for secure neighbour discovery and reliable data transmission through intermediate nodes. This protocol, involved in local monitoring- verifying that the neighbour hops are protected and the data packet is forwarded to the correct next hop, as indicated by the entity in the verification table.

T	L	ND	NC 16	Checksum	Code 32
Multiplex Id		Channel id		Client Id	Reserved
Source IP				Destination IP	
LC				LD	
Data (……..)					

Figure 3: M2-MAC Protocol Header Message

- T - The T bits indicate the type of message. It is set to 0 for data messages and 1 for control messages.
- L - When set, this indicates that the Length of current data field is present.
- ND – contains a monotonically in-creasing counter value for this data.
- NC - The sequence number expected in the next control message to be received.
- Checksum - The checksum of the packet.
- Code - Specifies the function to be performed.
- Multiplex ID - The packet multiplex ID identifies a particular connection within a channel.
- Channel ID - Identifies the channel to which a control message applies.
- Call ID - Identifies the user session within a channel to which a control message applies.
- Reserved - The X bits are reserved for future extensions. All reserved bits are set to 0 on outgoing messages.
- Source IP- IP address of the source node.
- Destination IP- IP address of the destination node.
- LC- This indicates that the length of control messages.
- LD- Length of total message (header + payloads) in octets.
- Data -Zero or more bytes of data as indicated by the Length. This field may contain one or more Options.

4.*3 M2-MAC Protocol for Mesh Network*

The M2-MAC protocols have most interesting feature is that all data packet sent absolutely on Intermediate nodes regarding routing decisions as each carries complete route traverses. When node requires route to a

particular destination, it broadcasts a ROUTE REQUEST packet. Each recipient node that has not seen this specific ROUTE REQUEST and has no knowledge about the required destination rebroadcasts this ROUTE REQUEST after appending its own address to it. If this ROUTE REQUEST reaches the destination or an intermediate node that has a route to the destination in its ROUTE CACHE, it send ROUTE REPLY packet containing the complete route from source to destination.

The M2-MAC protocol designates all available channels as control channel and REQ/ACK/RES mechanism for data transmission.

The proposed M2-MAC has the following new features:

All the available channels are designated as control channels and data channels on Channel Negotiation and Allocation (CNA) and Data Transmission (DT) sub-intervals are descript in [22]. An intelligent control channel allocation algorithm, which considers co-channel interference, is proposed at the first stage. It is able to achieve load balancing among all channels, and it minimizes co-channel interference.

a) The Algorithm for Control Channel allocation (ACCA) uses all available channels as control channels. This type of allocation can indicate which radio on each node should tune to which channel to exchange control messages.

b) At the second stage, a REQ/ACK/RES mechanism is proposed to realize dynamical channel allocation for mitigate misrouting and provide the data transmission mechanism in wireless mesh networks.

V. MITIGATION MISROUTING PACKET DROP OVER (M2-MAC) PROTOCOL

In this section, we propose M2-MAC protocol to enable the detection of stealthy packet dropping attacks, data transmission and particularly mitigating the misrouting.

5.1 Dynamic channel allocation for data transmission and mitigating misrouting

In M2-MAC, first the REQ/ACK/RES mechanism is used to allocate the channels for data transmission. All control messages are exchanged over the ACCA's resulting channels for mitigating misrouting. The second coordination stage describe by following steps:

Step 1: Once a beacon comes, if a source node (node S) has data pending for a destination (node D), S should check its $CRUS_S$ to find whether a radio and an available channel can be used for data transmission. If so, S waits for T_{DIFS} and a random exponential back off value, and then transmits a packet REQ (C_{hannel} R_{adio} $U_{tilization}$ $S_{tructure(S)}$) to M and broadcasts it to S's neighbours. If node S does not have data pending, then S must wait until the next beacon comes.

While the REQ process packet header incorporate with additional functionality and information. To collect the next-hop identity information, the forwarder of the REQ packet header attaches the previous hop's information ($S^{broadcast} \rightarrow ||S_i$ $||D_{id}||$ $REQ_{id}||A_{id}||M_{id}||$ Verification table|| Timestamp) and timestamp for calculate the possible maximum distance between S and D , when sending time of data packets.

Step 2: Once node D receives the packet REQ ($CRUS_S$), D has to check whether it has idle radios. If it does not, then D sends an acknowledgment message ACK (I_nV_{alid}) to S and broadcast it to D's neighbors to inform them that all radios on D are busy. If it does have idle radio, then D needs to select list of shortest channels in terms of priority for data transmission.

Step 3: when D receives the REQ packet, it verifies authenticity of source. Then D generates a route reply packet REP that contains ($D^{broadcast} \rightarrow ||D_{id}||S_{id}||REP_{id}||A_{id}||M_{id}||$Verification table||Timestamp). The REP continues to propagate using the reverse path of the corresponding REQ towards S. S will check the information carried by ACK. If it is N_{ull} or I_nV_{alid} or CH_k, S cancels the negotiation process and goes to step 1, if it is CH_k. Then S will check if this channel can still be used. If that is the case, S updates it's $CRUS_S$ and then broadcasts a reservation message RES (CH_k) across the network.

Then verifies the authenticity and calculates maximum possible time interval between S and D from the difference between sending time of data and receiving

time of data and assuming that the control packet travels with the speed of light. .

One must note that all the control messages, REQ, ACK, and RES, are transmitted over the allocated control channels from the first coordination stage. At this stage, ACCA is able to indicate the mapping relationship for which radio should be tuned to which control channel. Obviously, the hidden node problem can be alleviated in M2-MAC.

VI. CONCLUSION

We focused on analysing the ability of routing protocols to provide correct service in the presence of stealthy attack. This goal is achieved by M2-MAC coordination secure protocol resilient to misrouting failures caused by an adversary or group of malicious node. At the first coordination stage an intelligent control channel allocation algorithm, make all the available channels are designated as control channels and data channels on Channel Negotiation and Allocation (CNA) and Data Transmission (DT) sub-intervals. At the second stage, a REQ/ACK/RES mechanism is proposed to realize dynamical channel allocation for mitigate misrouting and provide the data transmission mechanism in wireless mesh networks.

VII. REFERENCES

[1]. http://pervasiveia.com/blog/cross- channel-definition

[2]. M. Zapata, N. Asokan, Securing ad hoc routing protocols, ACM Workshop on Wireless Secuirty (WiSe), September 2002, pp. 1–10.

[3]. Y. Hu, A. Perrig, D. Johnson, Ariadne: a secure ondemand routing protocol for ad hoc networks, in: ACM Annual International Conference on Mobile Computing and Networking (MOBICOM), September 2002, pp. 12– 23.

[4]. N. Borisov, I. Goldberg, D. Wagner, Intercepting mobile communications: the insecurity of 802.11, in: ACM Annual International Conference on Mobile Computing and Networking (MOBICOM), September 2002, pp. 180–188.

[5]. L. Buttyan, J.-P. Hubaux, Rational exchange—a formal model based on game theory, in: 2nd International Workshop on Electronic Commerce, November 2001.

[6]. K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M. Belding-Royer, A secure protocol for ad hoc networks, in: IEEE International Conference on Network Protocols (ICNP), 2002, pp. 78–87.

[7]. Y. Hu, A. Perrig, D. Johnson, Packet leashes: a defense against wormhole attacks in wireless networks, in: IEEE Annual Conference on Computer Communications (INFOCOM), 2003, pp. 1976–1986.

[8]. W. Stallings, "Cryptography and Network Security: Principles and Practice", Fifth Edition, Prentice Hall, 2010.

[9]. A. J. Menezes, P. C. V. Oorschot, and S. A. Vanstone, "Handbook of Applied Cryptography", CRC Press, ISBN: 0849385237, 1996.

[10]. C. Gandhi and M. Dave, "A Review of Security in Mobile Ad Hoc Networks", IETE Technical Review, ISSN: 02564602, pp.335-344, Vol. 23, No. 6, 2006

[11]. H. Yang, H. Luo, F. Ye, S. Lu, L. Zhang, Security in mobile ad hoc networks: challenges and solutions, IEEE Wireless Communications 11 (1) (2004) 38–47.

[12]. C. Siva Ram Murthy and B.S Manoj, "Ad Hoc Wireless Networks: Architectures and Protocols", Pearson Education, ISBN: 978-81-317-0688-6, 2006.

[13]. M. Jakobsson, S. Wetzel and B. Yener, "Stealth Attacks on Ad Hoc Wireless Networks", Proceedings of IEEE 58th Vehicular Technology Conference, pp.2103-2111, Vol.3, 2003.

[14]. Issa Khalil, saurabh bagchi, cristina N. rotaru, Ness . Shroff. " UNMASK: Utilizing neighbor monitoring for attack mitigation in multihop wireless sensor networks. Ad hoc netw (2009).

[15]. Issa Khalil, saurabh bagchi, MISPAR: Mitigating stealthy packet droping in locally monitores multi hop wireless Ad Hoc Networks, SecureCom 2008.

[16]. I. Khalil, S. Bagchi, and N. Shroff, "LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks," Proc. Int'l Conf. Dependable Systems and Networks (DSN '05), pp. 612-621, 2005.

[17]. IEEE 802.11a: Wireless LAM Medium Access Control (MAC) and Physical Layer (PHY) Specifications – Amendment 1: High-speed Physical Layer in the 5 GHz band". IEEE, 1999.

[18]. Marco A. Marsan, Daniele Roffinella. "Multichannel Local Area Network Protocols". IEEE JSAC, vol. SAC-1, no.5, November 1983. pp.885-897.
[19]. A. Nasipuri, J. Zhuang, and S.R. Das. "A Multichannel CSMA MAC Protocol for Multihop Wireless Network". IEEE Wireless Communications and Networking Conference (WCNC'99), 1999.
[20]. Elvino S. Sousa, and John. A. Silvester. "Spreading Code Protocol for Distributed Spread-Spectrum Packet Radio Networks". IEEE Transactions on Communications, Vol.36 No.3, March 1988. Page 272-281.
[21]. Ian F. Akyildiz , Xudong Wang , Weilin Wang Wireless mesh networks: a survey Broadband and Wireless Networking (BWN) Lab, School of Electrical and Computer Engineering, Received 1June 2004; received in revised form 1November 2004; accepted 20 December 2004.
[22]. Bingxuan zhao and shigeru shimamoto "Two stage coordination Mulyi-Radio Muli-Channel MAC Protocol for Wireless Mesh Networks", School of information and telecommunication, Tokyo,(IJCNC)volume3,No4,Jul2011.
[23]. http://www.javvin.com/protocols.