Available online www.jsaer.com

Journal of Scientific and Engineering Research, 2018, 5(3):467-472

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Novel Approach for Misbehavior Detection for MAC in Mobile ad hoc Network

Parul Rajput[1], Jitendra Singh Chouhan[2]

[1]M. Tech Scholar, Stream: Software Engineering, College: Aravali Institute of Technical Studies, Umarda, Udaipur

[2]Associate professor, Department of Computer Science & Engineering, Aravali Institute of Technical Studies, Umarda, Udaipur

Abstract Misbehavior of MAC layer due to malicious reasons can significantly degrade the performance in mobile ad hoc networks. In this paper we study to ameliorate the security and detect the time out attack, reduce the malignant node and amend the quality of service using proposed algorithms.

Keywords MANET, MAC 802.11, Misbehavior detection, RCCA, PSO, TMDA

1. Introduction

A Mobile Ad hoc Network (MANET) is a network of mobile devices that provides communication between mobile devices through wireless links without using any centralized control or fixed infrastructure [1]. The characteristic feature of MANET is the lack of any fixed infrastructure compared with the satellite or cellular networks. Networks are divided into two types predicated on the topology of the network, namely infrastructure network and infrastructure less network or Ad hoc Network [2]. In infrastructure network, wireless nodes are connected with the nearest Access Point (AP) that is within its communication radius. In infrastructure less network, a group of mobile nodes are connected with the radio links without any centralized control or AP. It is also known as peer-to-peer network or Ad hoc network. In ad hoc networks, mobile devices communicate with each other through a multi-hop route, using cooperating intermediary nodes. Each node in this network acts as a router and takes part in multi hop communication as shown in Figure 1.1.

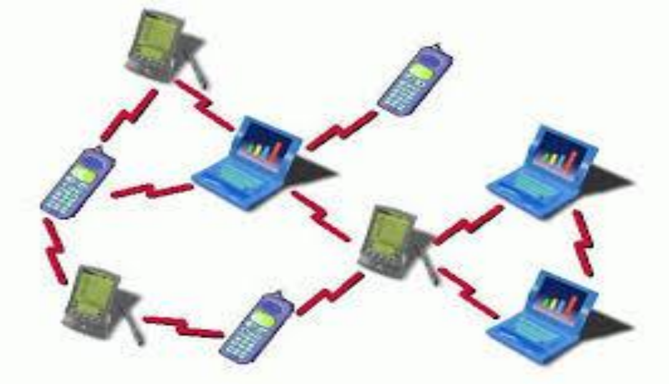

Figure 1.1: Mobile ad hoc networks

Each node should forward packets to its neighbouring nodes in order to communicate with far away nodes. Any node can join in the network or can leave the network without any constraint. This property of MANET makes it very flexible and robust and also it does not depend on a particular node as in an infrastructure network.

MANETs are being used in emergency search and rescue, military operations, to provide internet connectivity in conference environment and more recently in businesses (such as advertising and personal P2P networks).

2. IEEE 802.11 MAC PROTOCOL

IEEE 802.11 MAC uses two types of coordination function to access the wireless networks. Firstly, Distributed Coordination Function (DCF), which sanctions contention access for wireless channel and secondly, Point Coordination Function (PCF), which requires centralized APs. The architecture of the IEEE 802.11 MAC is shown in Figure 2.1. PCF is the upper sublayer and DCF is the lower sublayer in the MAC protocol. PCF is a contention free access protocol, which is controlled by centralized point coordinator to fortify authentic time traffic. The main drawback of PCF is that it will not work for MANET due to the central coordinator and withal it is not commonly fortified in commercial products.

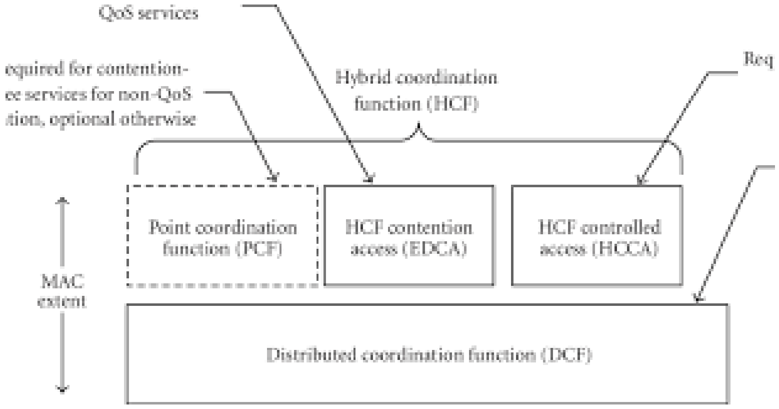
QoS services
equired for contention-
ee services for non-QoS
tion, optional otherwise
Hybrid coordination function (HCF)
Req
Point coordination function (PCF)
HCF contention access (EDCA)
HCF controlled access (HCCA)
MAC extent
Distributed coordination function (DCF)

Figure 2.1: IEEE 802.11 MAC architecture

DCF is an arbitrary access method, which uses Carrier Sensing Multiple Access with Collision Avoidance (CSMA/CA) to access and reduce the packet collisions. In CSMA/CA networks, a radio station which finds that the radio environment is available will commence to transmit only after desultory backoff procedure (Potorac 2009). Any node which wishes to transmit will first sense the channel to ken the status of the medium (diligent/idle). If the medium is diligent, the node defers its transmission until the medium is tenacious to be idle for a duration which is identically tantamount to DIFS. If the node is idle for DIFS time, it then enters into the backoff window or contention window. Backoff time is a desultory value which can be culled uniformly from the range 0 to CWmin-1, where CWmin is the minimum contention window size with a standard value of 32 and the maximum contention window size is set to 1024. When the channel is sensed idle, the backoff timer is decremented for every time slot and freezes when the medium is sensed diligent. When the backoff timer reaches 0, the node commences its next transmission. The node doubles the contention window for each unsuccessful transmission until it reaches the maximum value CWmax = 2mCWmin, where m is the maximum backoff stage with a standard value of 5. This is kenned as Binary Exponential Backoff (BEB) algorithm. This will reset to minimum contention window after each prosperous transmissions [3].

The backoff value is expressed by the following equation

Backoff Counter = INT (Rnd().CWmin)

where, Rnd() is a function that returns pseudorandom numbers uniformly distributed in (0, 1) [4] .

DCF defines two types of carrier sensing mechanism. First mechanism is called physical carrier sense, which is fortified by the physical layer. Second mechanism is virtual carrier sense, which is fortified by the MAC layer.

2.1.1. Basic Access Method

DCF includes both rudimental access method and an optional channel access method utilizing Request To Send / Clear To Send (RTS/CTS) exchanges. Rudimentary access mechanism is a two way handshaking method where only data and ACK are exchanged which is shown in Figure 2.2. When the transmitter transmits data to the receiver after Short Inter-Frame Space (SIFS) interval, the receiver replies with the ACK control frame. If ACK is not received by the sender within the designated ACK_Timeout period then, the frame is surmised to be disoriented and schedules the retransmission.

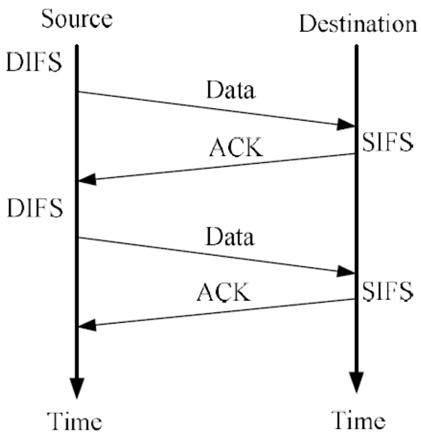

Figure 2.2: IEEE 802.11 basic access handshake

2.1.2. RTS-CTS Mechanism

In RTS/CTS access method, when the node wants to transmit a data frame it should wait until the channel is sensed idle for DIFS time and backoff time. Then only the node can transmit short RTS control frame in lieu of data frame. After a SIFS interval the receiver replies with the short CTS control frame. This RTS/CTS exchange ascertains that both the sender and receiver are yare to transmit and receive the frames which are shown in Figure 2.3.

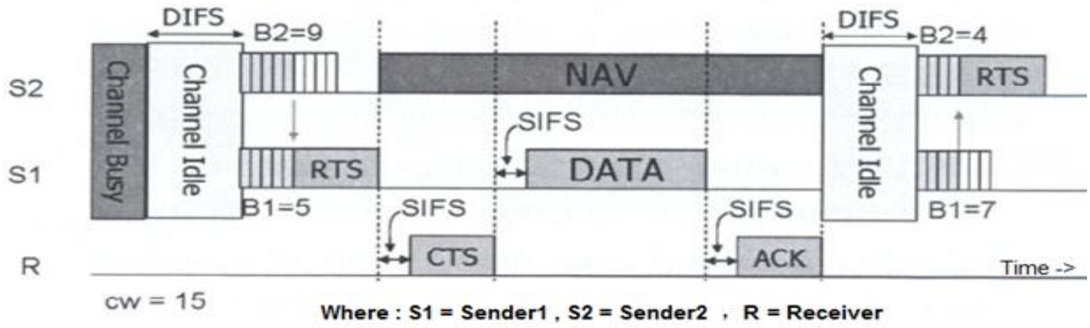

Figure 2.3: IEEE 802.11 RTS/CTS mechanism

The RTS and CTS frames both contain details about the length of the frame to be transmitted. Neighbouring nodes which overhear the RTS and CTS control packets will update their Network Allocation Vector (NAV).

NAV is a timer which is included along with the duration field of RTS, CTS control frames. When the NAV timer becomes, neighbouring nodes can commence their transmission, otherwise it would be silent. Now the sender sends data packets after the SIFS interval. The receiver replies with ACK to substantiate the reception of the data packets. SIFS period is shorter than the DIFS period, which guarantees perpetual RTS+CTS+DATA+ACK exchange [5].

2.1.3. Misbehaving Techniques

In the Data link layer, in order to achieve an operational point in the network, all the CSMA/CA schemes surmise that all participants should stringently follow the protocol designations. However, especially in the presence of autonomous nodes this postulation may not always be valid. Lamentably, there are sundry ways in which a station can gain advantage by not adhering to the protocol guidelines like:

Culling diminutive backoff values: A selfish node can optate a more minuscule value in lieu of culling desultorily. Not doubling CW after collision: A node may not invoke the collision instauration procedure after collision. Thus, the node would always be culling its backoff values from [0, CWmin], thereby using values for backoff.

Manipulating the NAV value: If a node increases this value, it can assure that all other agents will remain idle even after the terminus of current transmission. Not corroborating to the DIFS and SIFS intervals: This comportment will increment the chances of getting access to the medium. Magnify the value of the duration field in RTS or DATA packets such that the receivers keep silence for a period more sizably voluminous than the authentic transmission time. As a result, if the cheater node has more packets to send, it gets more chance to access the medium, as it commences counting down its backoff afore its neighbours.

When the channel is found to be idle, it transmits afore the required DIFS time slots elapses, i.e. the misconducting node waits for a shorter period called S-DIFS (Short-DIFS).

3. Related Work

Baker & Ephremides [7] proposed identifier-predicated clustering algorithm kenned as lowest-ID. It assigns a unique ID to each node and whenever an incipient node with a lowest ID appears, the cluster-head is superseded.

Gerla & Tsai [7] proposed the clustering algorithm for highest connectivity. It is a wireless adaptive mobile information systems with multi-cluster, multi-hop packet radio network architecture. In this technique the degree of nodes is calculated, which is the number of neighbours of a given node. During election procedure, each node broadcasts its identifier. After computing its degree, the node having the maximum degree becomes the cluster-head.

Kyasanur & Vaidya [8] have proposed the MAC layer misconduct through the modification of the IEEE 802.11 MAC protocol, in order to detect and penalize the selfish misconduct. Here the receiver assigns back off value to the sender utilizing RTS and ACK control packets. The sender utilizes this assigned back off value in the next transmission.

Lolla et al [9] have modified the IEEE 802.11 MAC protocol and has proposed the method to detect the MAC layer backoff timer breaches in MANETs. In this method, the arbitrary number engenderer state exchanges the arbitrary number engendered to every neighbour. After that wilcoxon rank sum test is utilized to detect the misconduct. This test utilizes the fine-tuned sample size to compare the distinction between analytically computed samples and the observed sample size. The disadvantage of this approach is the utilization of the fine-tuned sample size to detect the misconducting node and withal it does not handle collusion between nodes.

Kyasanur & Vaidya [8] have proposed the MAC layer misconduct through the modification of the IEEE 802.11 MAC protocol, in order to detect and penalize the selfish misconduct. Here the receiver assigns back off value to the sender utilizing RTS and ACK control packets. The sender utilizes this assigned back off value in the next transmission.

Lolla et al [9] have modified the IEEE 802.11 MAC protocol and has proposed the method to detect the MAC layer backoff timer breaches in MANETs. In this method, the arbitrary number engenderer state exchanges the arbitrary number engendered to every neighbour. After that wilcoxon rank sum test is utilized to detect the misconduct. This test utilizes the fine-tuned sample size to compare the distinction between analytically computed samples and the observed sample size. The disadvantage of this approach is the utilization of the fine-tuned sample size to detect the misconducting node and withal it does not handle collusion between nodes.

Predicated on the RTS/CTS scheme, many MAC protocols are proposed to eschew data collision [10]. The prosperity of the RTS transmission depends mostly on the performance of these protocols. Some research's make utilization of the concept of supplemental channel(s) to alarm itself for transmission, in order to preclude others interference.

However, seldom in the literature it was proposed to obviate from the RTS collisions. Park & Sivakumar [11] considered traffic load which evaluated the collision effect on network performance. All of the above protocols pointed out that contention-predicated MAC protocols are facile to encounter RTS collisions, especially in cumbersomely hefty traffic load and subsequently, degrades the network throughput and performance. Moreover, the demeanor of RTS/CTS handshaking analysis results in the probability of RTS collisions in any contention-predicated scheme to be higher than subsisting.

4. Proposed Methodology

In this paper, in order to achieve security in the network three novel methods are designed. The first method mainly contributes to the detection and aversion of TimeOut (TO) attack. The second method utilizes the

Particle Swarm Optimization (PSO) algorithm where each node culls an optimal value to eschew the nodes. The third method RTS-CTS Collision Avoidance Algorithm (RCCA) averts the collision during communication.

A. Timeout Misbehavior Detection Algorithm (TMDA): Timeout Misbehavior Detection Algorithm (TMDA) is developed to detect TO attack of sender and receiver misconduct. Initially the expected TOCTS value is calculated. Then during frame transmission, the actual TOCTS value is calculated. By comparing both the values, the TMDA algorithm decides whether it is sender misbehavior or receiver misbehavior. After detecting the misbehaving node, rectification procedure has been carried out. The performance of the TMDA algorithm is analyzed in terms of throughput, delay, PDR, misdetection and correct detection ratio. From the results, the TMDA algorithm is compared with IEEE 802.11 MAC protocol which gives better throughput, PDR and correct detection ratio. Misdetection ratio, delay and jitter are reduced in TMDA algorithm when compared with IEEE 802.11.

B. Particle Swarm Optimization (PSO) algorithm: The fundamental conception behind PSO method is to amend the security by detecting and penalizing the misbehaving nodes. This amends the throughput and PDR while decrementing the delay, jitter and number of RTS/CTS collisions. Predicated on these conceptions, an incipient method is developed utilizing particle swarm optimization technique to reduce the number of misbehaving nodes. After implementing the PSO algorithm, the throughput and packet delivery ratio is incremented while delay is decremented.

C. RTS-CTS Collision Avoidance Algorithm (RCCA): A RCCA model is developed to avert the collisions in two hop neighbors. By using this algorithm, number of RTS-CTS collision is reduced considerably compared with the IEEE 802.11 MAC protocol. During collisions, selfish nodes endeavor to optate diminutive back off value to get more access than the well comported nodes. Hence indirectly the selfish misbehaving nodes are obviated. Here the RTS-CTS collisions are eschewed by introducing Collision Avoidance Packet (CAP). CAP contains Active Neighbor Bit (ANB), which gives information about whether any communication is going on within the transmission range. Predicated on this information, nodes decide themselves to send the data packet or to stop the communication. The performance of the RCCA algorithm is tested with Network Simulator - 2 (NS-2). Predicated on the results, the throughput and packet delivery ratio are amended compared with the IEEE 802.11 MAC protocol. Delay and number of RTS-CTS collisions are decremented compared with the subsisting MAC protocol.

5. Conclusion and Future Scope

MAC layer misbehavior in IEEE 802.11 networks can lead to performance degradation in MANET. Current work has mainly focused on the misbehaving nodes and their impact on the degradation of MANET performance.

For future work, we will explore the algorithm Time out Misbehavior Detection Algorithm (TMDA).

Reference

[1]. Perkins, CE & Royer, EM 1999, 'Ad hoc on-demand distance vector routing', Proceedings of the 2nd IEEE workshop on mobile computing systems and applications, New Orleans, pp. 90-100.

[2]. Kyasanur, P & Vaidya, NH 2003, 'Detection and handling of MAC layer misbehavior in wireless networks', Proceedings of the international conference on dependable systems and networks, pp.173-182.

[3]. Tang, J, Cheng, Y & Zhuang, W 2012, 'Real-Time Misbehavior Detection in IEEE 802.11 Based Wireless Networks: An Analytical Approach', IEEE Transactions on Mobile Computing, IEEE computer Society Digital

[4]. Cagalj, M, Ganeriwal, S, Aad, I & Hubaux, JP 2004, 'On Cheating in CSMA/CA Ad Hoc Networks', Technical Report IC/2004/27, EPFLDI- ICA.

[5]. Konorski, J., 2007. A station strategy to deter backoff attacks in IEEE 802.11 LANs. J. Discrete Algorithms, 5: 436-454.

[6]. Baker, DJ & Ephremides, A 2003, 'The architectural organization of a mobile radio network via a distributed algorithm', IEEE Transactions on Communications, vol. 29, pp. 1694-1701.

[7]. Gerla, M & Tsai, JTC 1995, 'Multi-cluster, mobile, multimedia radio network, Wireless Networks 1', vol. 3, pp. 255-265.

[8]. Kyasanur, P & Vaidya NH 2005, 'Selfish MAC layer misbehavior in wireless networks', IEEE Transactions on Mobile Computing, vol. 4, no. 5, pp. 502-516.

[9]. Lolla, VN, Law, LK, Krishnamoorthy, SV, Ravishankar, C & Manjunath, D 2006, 'Detecting MAC layer back-off time violations in MANETs', proceedings of international conference on distributed computing systems(ICDCS'06), pp.63

[10]. Garcés, R & Garcia-Luna-Aceves, JJ 1996, 'Floor acquisition multiple access with collision resolution', Proceedings of the ACM international conference on mobile computing and networking (MOBICOM) conference, USA, pp. 187-197.

[11]. Park, SJ & Sivakumar, R 2002, 'Load sensitive transmission power control in wireless ad-hoc networks', Proceedings of the IEEE global telecommunications conference (GLOBECOM), pp. 42-46.