Enhance Security Model of MANET with Advance MAC Protocol Using NAV Setting

Vinay Kumar Pandey[1], Rajni Kant Pandey[2], Alka Kaushik[3], Sumiran Daiya[4]

[1]*Assistant Professor, Computer Science Department, SKITM, Haryana. INDIA*

[2,4] *M.Tech Scholar, Department of ECE, Haryana. INDIA*

[3] *M.Tech Scholar, Department of CSE, Haryana. INDIA*

Abstract –**Mobile ad- hoc Network is used on that place where the installation of Network setup is not possible using wire & base infrastructure like centralize server. In this situation the up to date technologies apply called ad hoc network. The migration form wired network to wireless network has been a worldwide trend within the few decades. The various type of the upgrade wireless networks, Mobile Ad hoc Network is one of the needful and separate application like in any rescue operation, battlefield & all ad-hoc network. To achieve the good throughput, cooperative communication utilizes nearby terminals to broadcast the overhearing information, has a great potential to improve the transmitting efficiency in mobile ad hoc networks. Here we are explaining a trust concept using Finite state machine based on a MAC protocol which support the avoidance of packets collision using NAV setting in both data link layer and network layer (routing & link layers) of Mobile ad hoc networks(MANETs).**

Keywords - **AdvanceNAV setting, MAC protocol, Security of MANET, 802.11 WLAN standards, PCF & DCF.**

I. INTRODUCTION

Fundamental access mechanism is carrier sense multiple access with collision avoidance with binary exponential back off similar to IEEE 802.3 standard with some significant exceptions. Career Sense Multiple Access with Collision Avoidance is used as listen before talk access mechanism. When there is a transmission in the medium the station will not begin its own transmission. This is the Career Sense Multiple Access portion of the access mechanism. If there is a collision and the transmission corrupted the function of the access mechanism works to ensure the correct reception of the information broadcast on the wireless medium may effectively identify the various types of active & passive attacks which occur at the 802.11 WLAN MAC protocol in time and with low overhead using the binary exponential back off algorithm. It will also increase the actual retry counter related with the associated frame. The random number gives output from this algorithm i.e. uniformly distributed in arrangement called the contention window, the size of which doubles with every attempt to transmit that is deferred, until a maximum size is reached for the range. Once a transmission is completely transmitted the range is reduced to its minimum value for the other transmission. It is extremely unusual for a wireless device to be able to receive and transmit signal simultaneously. The IEEE802.11 MAC protocol uses collision avoidance rather than the collision detection of IEEE 802.3. It is also usual for all wireless devices in LAN to be able to communicate directly with all other devices. For this reason, IEEE802.11 MAC implements a network allocation vector setting [14].

II. MEDIUM ACCESS CONTROL (MAC) FRAME FORMAT

Each frame consists of

1. A MAC Header: frame control, duration, address, and sequence control information
2. Avariable length framebody
3. A frame checks sequence(FCS), contains IEEE 32-bit cyclic redundancy code(CRC)

The General Frame Format of MAC Contain Nine fields including FCS 4 bytes.

A. *Medium Access Control(MAC) Function:*

Reliable data delivery, fairly control access to the shared wireless medium &protect the data that it delivers. In the IEEE 802 reference model of computer networking, the medium access control or media access control (MAC) layer is the lower sublayer of the data link layer (layer 2) of the seven-layer OSI model.

The MAC protocol encapsulates a SDU (payload data) by adding a 14 byte header (Protocol Control Information (PCI)) before the data and appending an integrity checksum, The checksum is a 4-byte (32-bit) Cyclic Redundancy Check (CRC) after the data. The entire frame is preceded by a small idle period (the minimum inter-frame gap, 9.6 microsecond (μS)) and a 8 byte preamble (including the start of frame delimiter).

Ethernet is an example of a protocol that works at the Media Access Control layer level..

B. *Control Frame of MAC:*

MAC accepts MSDUs from higher layers and adds headers and trailers to create MPDU. The MAC may fragment MSDUs into several frames, increasing the probability of each individual frame being delivered successfully.

Header+MSDU+Trailer contain information addressing information IEEE 802.11specific protocol information, for setting the NAV frame check sequence for verifying the integrity of the frame.[14]

- *RTS of MAC*- it contains 20bytes long which consist of Frame Control Field, Duration field of RTS & individual address with TA and Frame Check Sequence. The purpose is to transmit the duration to stations in order for them to update their NAV to prevent transmissions from colliding with the data or management frame that is expected to follow. Duration information conveyed by this frame is a measure of the amount of time required to complete the four-way frame exchange.

Duration Time = CTS + Data/management frame+ ACK+ 2 SIFS

- **CTS of MAC-**CTS consist 14bytes

a. Frame Control Field, Duration/ID Field
b. RA, individual MAC address
c. FCS for updating the NAV.
Duration Time =Data frame+ ACK + 1 SIFS

- *ACK of MAC*: it contains 14 bytes

a. Frame Control Field
b. Duration/ID Field (MS): Duration is zero. The value of the duration information is the time to transmit the subsequent data &management frame, an ACK frame, and two SIFS intervals, if the acknowledgement is of a data or management frame where the more fragments subfield of the frame control field is one.
c. RA: individual address. RA is taken from the address 2 field of data, management or PS-Poll frame.
d. FCS: The purpose of this frame is two-fold. First, the ACK frame transmits an acknowledgement to the sender of the immediately previous data, management, or PS-Poll frame that the frame was received correctly. Second, the ACK frame is used to transmit the duration of information for a fragment burst as in CTS.[14]

C. Network Allocation Vector Setting:

It is describing under the MAC exchange protocol. It is Extremely unusual for a wireless device to be able to receive and transmit simultaneously, the IEEE802.11MAC uses collision avoidance rather than the collision detection of IEEE 802.3.Itisalsounusual for all wireless devices in LAN to be able to communicate directly with all other devices. For this reason IEEE802.11MAC implements a network allocation vector.

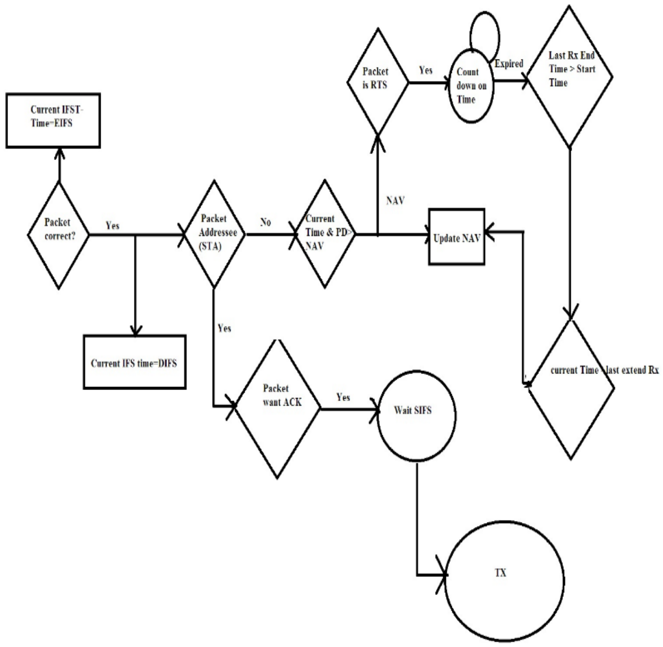

Fig: 1 Finite State representation of NAV setting.

III. MANAGEMENT FRAME

IEEE 802.11w-2009 is an approved amendment to the IEEE 802.11 standard to increase the security of its management frames.

Management frames include Frame Control Duration, Address 1, 2, and 3, Sequence control, Frame body, Element ID Length Information (variable length) Frame check sequence (FCS) fields.

Beacon- A beacon is an intentionally conspicuous device designed to attract attention to a specific location.

Beacons can also be combined with semaphoric or other indicators to provide important information, such as the status of an airport, by the colour and rotational pattern of its airport beacon, or of pending weather as indicated on a weather beacon mounted at the top of a tall building or similar site. When used in such fashion, beacons can be considered a form of optical telegraphy.

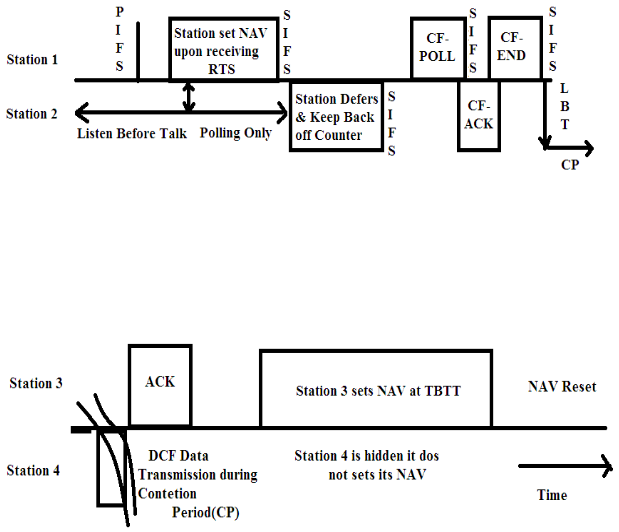
Station 1
P I F S
Station set NAV upon receiving RTS
S I F S
CF- POLL
S I F S
CF- END
S I F S
Station 2
Listen Before Talk
Polling Only
Station Defers & Keep Back off Counter
S I F S
CF- ACK
L B T
CP
Station 3
ACK
Station 3 sets NAV at TBTT
NAV Reset
Station 4
DCF Data Transmission during Contetion Period(CP)
Station 4 is hidden it dos not sets its NAV
Time

Fig: 2 PCF Operations

- *Virtual Carrier Sensing:*

VCS informs stations about ongoing or planned transmission. All stations that are not in power-save mode monitor the Wireless Medium (WM). Stations retrieve risers- constantly. If the duration field is present, stations set their Network Allocation Vector to the according value. The NAV work as count down times. The timer has value different than zero, V-CS indicates a busy WM. The value of NAV updated at any time

IV. FUTURE WORK

The design of the Network can be further expand in future with order to

- Enhance the Centrally Controlled Access Mechanism in MANET.
- Searching update setting like NAV for good control access to the shared wireless medium
- Enhance Capability of protecting the data when delivering via MAC using NAV.

V. CONCLUSION

The above discussion [1-3] Detect & activate the network using advance beacon interval technique that employed at the network layer of MANET for exact time setting between nodes. The advance NAV setting senses the route and update path between nodes automatically, using value. So it introduces a number of significant advantages since it can effectively detect all attacks in real time and without any communication overhead, it is resilient to the dynamic topologies that are common in Mobile ad hoc networks & its deployment.

REFERENCES

[1] Pandey V.K, “Enhance security of MAC protocol in MANET using Trust based engine” IEEE XploreMobile Computing vol. 10, no. 2, pp. 291-296, Mar. 2015.

[2] V. K Pandey, Harvir Singh, “Enhanced Secure Routing Model for MANET” in proceedings of the 8th International Conference on ITCSE, CS & IT 07, pp. 37–44, 2012.

[3] B. Kim, “OFDMA-Based reliable multicast MAC protocol for Wireless Ad-hoc Network”, ETRI Journal, vol. 31, no. 1, Feb. 2009.

[4] Huang, "Unlinkability Measure for IEEE 802.11 based MANETs," IEEE Transactions on Wireless Communications, no. 2, pp. 1025-1034, Feb 2008.

[5] Xi Zhang, and Hang Su, “CREAM-MAC: Cognitive Radio-Enabled Multi-Channel MAC Protocol Over Dynamic Spectrum Access Networks,” IEEE Transactions on Signal Processing, vol. 5, no. 1, February 2008.

[6] Tarag Fahad &Robert Ask with “A Node Misbehavior Detection Mechanism for Mobile Ad-hoc Networks”, in proceedings of the 7th Annual Post Graduate Symposium on The Convergence of Telecommunications, Networking and Broadcasting, June 2006.

[7] F. Li, K. Wu, K. Leung, and Q. Ni, “On Optimizing Back Off Counter Reservation and Classifying Stations for the IEEE 802.11 Distributed Wireless LANs,” IEEE Trans. Parallel and Distributed Systems, vol. 17, no. 7, pp. 713-722, July 2006.

[8] J. Choi, S. Choi, and C. Kim, “EBA: An Enhancement of IEEE 802.11 DCF via Distributed Reservation,” IEEE Trans. Mobile Computing, vol. 4, no. 4, pp. 378-390, July/Aug. 2005.

[9] S. Kim, Y. Kim, S. Choi, K. Jang, and J. Chang, “A High Throughput MAC Strategy for Next-Generation WLANs,” Proc. IEEE Symp. World of Wireless, Mobile and Multimedia Networks, 2005.

[10] S. Medidi& S. Gavini, “Detecting Packet Dropping Faults in Mobile Ad-hoc Networks,” In Proc. of IEEE ASILOMAR Conference on Signals, Systems and Computers, volume 2, pp. 1708–1712, 2003.

[11] S. Medidi& R L Gris, “Malicious Node Detection in Ad-hoc Wireless Networks,” In Proc. SPIE AeroSense Conference on Digital Wireless Communications, volume 5100, pp. 40–49, April 2003.

[12] J. Y. Le Boudec& S Buch. “Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks.” In Proceedings of the Parallel, Distributed and Network-based Processing, pages 403–410, Jan 2002.

[13] M. Royer, S. J. Lee, and C. E. Perkins, “The effects of MAC protocols on ad hoc networks communication,” Proceeding. Of IEEE WCNC, pp. 543-548, Sep. 2000.

[14] Mustafa Ergen “IEEE 802.11 Tutorial” ergen@eecs.berkeley.eduUniversity of California Berkeley June 2002

[15] Margaret Rouse “Media Access Control layer (MAC layer)” http://searchnetworking.techtarget.com/definition/Media-Access-Control-layer

[16] Media Access Control layer (MAC layer) http://www.erg.abdn.ac.uk/users/gorry/course/lan-pages/mac.html

[17] www.en.wikipedia.org