Volume 8, No. 3, March – April 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
REVIEW ARTICLE
Available Online at www.ijarcs.info

Security Mechanism for CSMA/CD Networks: A Survey

Shubham Singh and Nensi Kansagara
Institute of Technology
Nirma University, Ahmedabad, Gujrat, India

***Abstract*:** In this paper we study about security against various malicious attacks. In this we also represent some known feasible attacks. We also get information about secured communication for different mechanism which provide a secrecy, security and authentication to most of security issues. In some logical section we learn about an active repeater in CSMA/CD for network comparison for data transmission between two addresses. If no match occurs, the logic section controls the transmitter so that the transmitter switches from transmitting the data packet to the clock signal. For bidirectional routing message received from wired network and send it to wireless network. At the end we get comparison result for transmitted message to the received message to find if a collision has occurred.

Keywords: CSMA/CD, Sensor Network, DTDV protocol.

I. INTRODUCTION

Using CSMA/CD concept in automotive electronics we get appropriate outputs for car, vehicle, like breaks, engine control and airbags. Using ESP (Electronic Stability Program) we modified car system and deep inventions in driving behaviour of vehicles. The present invention is directed to local area data communications networks, and in particular to active repeater units for use in star-configured carrier sense medium access collision detection (CSMA/CD) type networks having the characteristic that all traffic on the network medium can be seen by any station connected to the network.

Carrier sense multiple access with collision detection (CSMA/CD) is a media access control[4] method used most no-table in local area networking using early Ethernet technology. Here we discussed about speech coding which is basically transmission of few binary digits. We considered some speech coding techniques like wave forming, linear predictive coding etc. In speech coding translation process begins by establishing a voice communication channel between the service mobile device and voice recognition server. In CSMA/CD we used power computing gor transmission of light weighted data over a network which provide us a powerful computing into a network .Because it has many reasons one of them is they are self-configuring and other they covers large area of application like in hospitals, military, police and minor application like playing a game. Here each and every node acts as a router so traffic goes through it. Every node is self-configuring, so it can maintain itself in network work on a portable network.

In a network, we connect through the radio frequency or maybe infrared frequency in wireless network between two Nodes while in a wired network we connected through net-work. Other reason is for popularity of CSMA/CD is, now a days mobile nodes are very cheap, powerful and openly available in large stock in market into reality of Ad-hoc network. Into this we share a one common channel that is DTE channel. Which uses carrier sense Multiple Access with Collision.

CSMA/CD is now a day is very popular because of its dynamic nature and its quick user responsiveness [2]. Ad-hoc network now a days very popular due to interoperability of mobile nodes and communication between them without any further networking infrastructure. For communication and information exchange purpose it uses various protocols, but we mainly categorize them in to three protocols, 1) proactive 2) reactive 3) hybrid. From these many protocol CSMA protocol is more popular among all because it is quite efficient and give more throughput compare to other protocols. In MANET many loopholes are there which can breaks the security, one of them is sinkhole attack. In this type intruder node tends to attracts all the network traffic towards it and disclose the communication. In this paper I try to propose algorithm which prevents sinkhole attack [7].

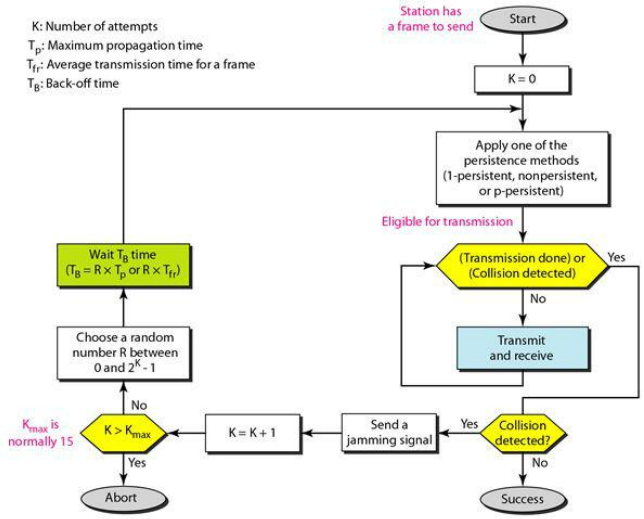

Fig. 1.Multiple Access Wireless Channel Diagram [11]

In general, CSMA/CD might be depicted as takes after: From all protocol CSMA protocol is most usable protocol. Because it is simple and efficient. The security issues in these protocols

are very critical. Here when nodes want to communicate beyond its boundary then it have to communicate with all other node by an intermediate node, these is where

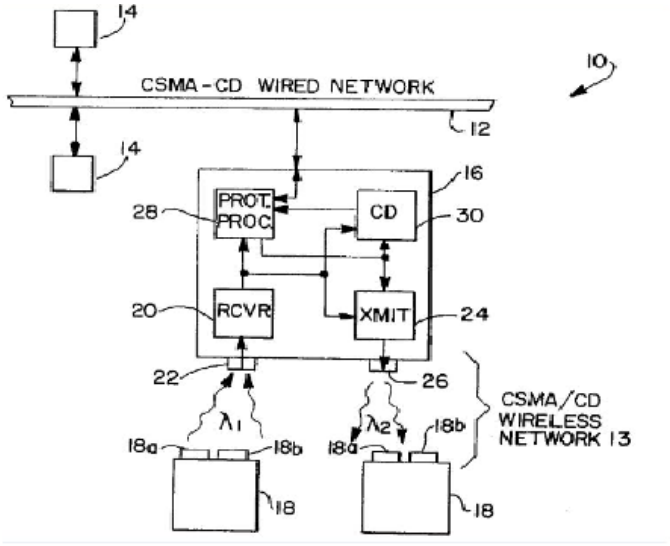

Fig. 2. CSMA/CD wired network [5]

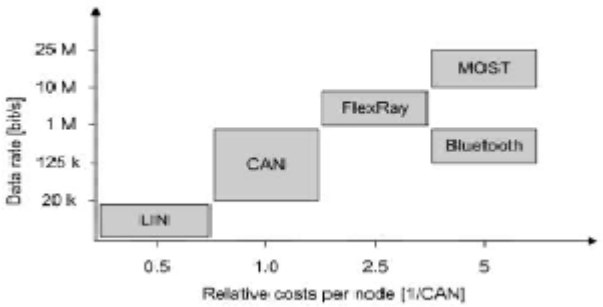

Fig. 3. Data Rates and Relative Cost [1]

Variability remains and various kind of attack possible like flooding and wormhole. Sinkhole attack is one of critical attacks that can be on DTE. In sinkhole attack one malicious node tries to attract all traffic towards it by broadcasting wrong routing information in network and modify or damage the content of packet. Attacks are categorize in to two subclasses, passive and active attacks, in which the traffic are observe and modified according to attack.

As mention earlier CSMA/CD is easier and efficient protocol and it uses limited bandwidth. Actually CSMA is combination of DTE and DTDV protocol. It takes route discovery from DTE by broadcasting destination and from it takes parotic update, sequence number and routing table mechanism [6]. The main difference between CSMA/CD and DTE IS does not include source route to every packet thus it reduce so much overhead but disadvantage is for packet update it requires more bandwidth.

II. AUTOMATIVE VEHICLE SYSTEM

Now a days we are using wide variety of vehicles for com-medication system which is already in automotive area. Which provide us variety of services and so many applications for mechanism services.

For network spanning communication, automotive bus systems require appropriate bridges or gateways processors to transfer messages among each other despite their die rent physical and logical operating properties. Channel fading in wireless network where we get reverse link data transmission in network while here in fading we used link between mobile terminal and base station so we get fast fading into channel [3] Which improve our network efficiency and redundancy for improving our results.

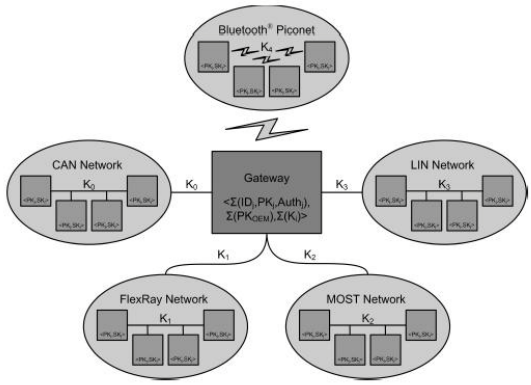

Fig. 4. Secure wireless communication [1]

As we mentioned earlier that this protocol maintains a table where it specify each path to destination and neighbour. Whenever new request comes node checks it routing table whether shortest path available or not, if yes it send route replay. Here destination send CSMA/CD message to source via unicast way, that means in which way it comes the same way it replay. Other scenario is initially it broadcast to all its neighbour, if some intermediate node have shortest path to destination then it replay from there to source that shortest path found.

III. SECURITY FEATURE

It provide an security feature for the ports of an active repeater unit, in a network operating under the carrier-sense-medium access/collision-detection protocols, which alters data packets received and retransmitted by the active re pester unit so that the retransmitted data packets are only transmitted through ports attached to data stations to which the data packets are addressed, while output ting a spurious carrier signal through the other active repeater ports.

It is another object of the present invention to perform a data packet? Altering operation in real-time, without data-packet-buffering so as not to adversely affect the topology of the network [9].

It is a further object of the present invention to provide active repeater ports which are selectively operable between a filtering mode where transmitted data packets are send, and a learn

mode where the address of the data station attached to a port is stored in a memory of that port for use in the faltering mode. To achieve the foregoing and other objects, and to overcome the shortcomings discussed above, a logic section is provided on each active repeater port for comparing the destination address of a data packet re transmitted by the active repeater unit with the address of the data station attached to that port to determine whether a match occurs between these two addresses. Each ports transmitter receives the retransmitted data packet and a spurious carrier signal while the logic section is determining whether an address Match occurs. The transmitter transmits the data packet to its corresponding data station until the logic section makes its match determination. If a match occurs between the destination address of the retransmitted data packet and the address of the data station attached to that port, the logic section controls the transmitter so that the transmitter continues to transmit the data packet to its data station. If no match occurs, the logic section controls the transmitter so that the transmitter switches from transmitting the data packet to transmitting the spurious carrier signal.

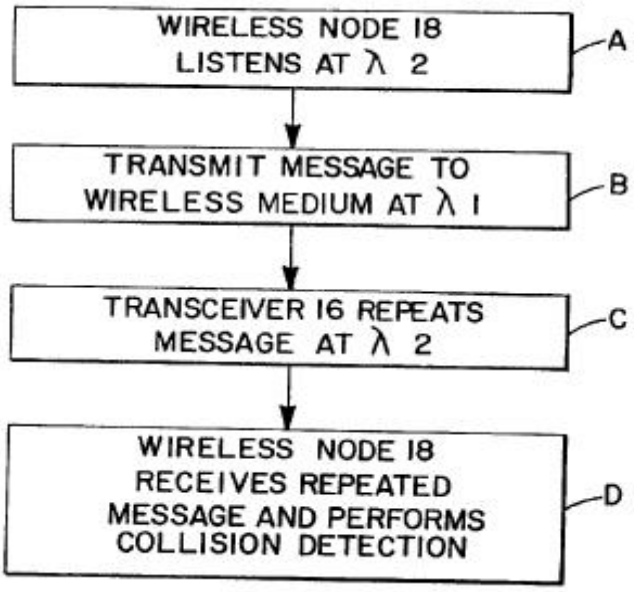

Fig. 5. Sequence of steps for transferring the packet of data over the wired/wireless CSMA/CD network [5].

In CSMA sinkhole attack is possible by modifying sequence number in CSMA/CD. Malicious node generate higher sequence number then source node and higher sequence number means is path is most fresh and more recent. Sinkhole node gets the sequence number of source and increase its own sequence number and send bogus REQ to all its neighbourhood. By this it is successfully draw all traffic towards it. Due to higher sequence number all nodes thinks that this route is more fresh and better.

In CSMA/CD protocol our approach can work well. An algorithm describe here is not only detect the sinkhole node but take necessary action. Through this approach we can in-crease our PDR (packet delivery ratio) too [8]. Thus this approach is very useful.it provide a better security into network using this protocol.

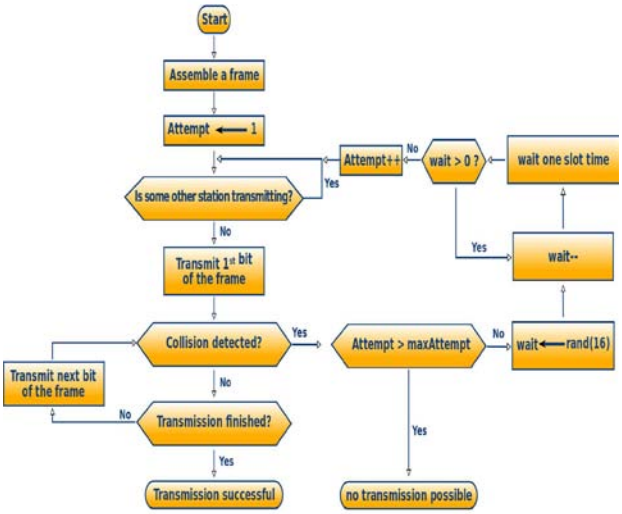

Fig. 6. Carrier Sense Multiplication [10]

IV. CONCLUSION

In this work we represent current and future communication system for CSMA/CD in vehicle system. In some time using multimedia vehicle concept we get wireless communication for most modern automobiles. In future automotive vehicle system provide very high secure, adaptive, technical, organized and financial expenditures have to be arranged today already.

V. REFERENCES

[1] R. Canetti, J. Garay, G. Itkis, D. Miccianicio, M. Naor, B. Pinkas. Multicast Security: A Taxonomie and Some Ecient Constructions. In Proceedings of IEEE INFOCOM '99, New York, USA , March 1999.

[2] R. Kraus. Ein Bus fr alle Flle. In Elektronik Automotive 01/2002.

[3] C. Paar. Eingebettete Sicherheit im Automobil. In Konferenz Embedded Security in Cars (ESCAR), Kln, November 2003

[4] Broch, Josh, et al. "A performance comparison of multi-hop wireless ad hoc network routing protocols." *Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking*. ACM, 1998.

[5] Hortensius, Peter Dirk, and Haaken B. Winbom. "Transceiver for extending a CSMA/CD network for wireless communication." U.S. Patent No. 5,917,629. 29 Jun. 1999.

[6] Thompson, Geoffrey O. "Hub privacy filter for active star CSMA/CD network." U.S. Patent No. 5,251,203. 5 Oct. 1993.

[7] Bonab, Tahmineh Haddadi, and Mohammad Masdari. "Security attacks in wireless body area networks: challenges and issues." *ACADEMIE ROYALE DES SCIENCES D OUTRE-MER BULLETIN DES SEANCES* 4.4 (2015): 100-107.

[8] Chae, Chang-Joon, Elaine Wong, and Rodney S. Tucker. "Optical CSMA/CD media access scheme for Ethernet over passive optical network." *IEEE Photonics Technology Letters* 14.5 (2002): 711-713.

[9] Wolf, Marko, André Weimerskirch, and Christof Paar. "Secure in-vehicle communication." *Embedded Security in Cars*. Springer Berlin Heidelberg, 2006. 95-109.

[10] https://upload.wikimedia.org/wikipedia/commons/thumb/3/37/CSMACD-Algorithm.svg/800px-CSMACD-Algorithm.svg.png

[11] https://image.slidesharecdn.com/aloha1-110120222230-phpapp02/95/aloha-26-728.jpg?cb=1391395148.