Abstract

The exponential growth of wireless network in recent years has brought some major research issues that include a fair share of the available bandwidth, quality of service (QoS) and control of misbehaving traffic nodes/sources. However, in wireless networks, including cellular, Ad Hoc, and sensor networks, that are based on a shared medium and often contention-oriented protocols, these issues have not been fully addressed. Most wireless networks are based on IEEE 802.11x standards which provide public wireless access to the Internet. The medium access control (MAC) in IEEE 802.11 uses a distributed contention resolution mechanism for sharing the channel. If the MAC protocol is manipulated or misused, then the consequences can be overwhelming, such as the disruption of the whole network. A selfish/cheater node [10] can manipulate the MAC protocol in different ways to gain access to the channel resulting in some cases of starvation of other nodes in the same network. The manipulation of the MAC layer protocol is hidden from the upper layers, and can be further enhanced if combined with more violations from these upper layers of the ISO/OSI Model. In wireless networks i.e. IEEE 802.11, all nodes contending to access the medium made-up to follow the rules of the Medium Access Control (MAC) sub layer. As the number of nodes increases; the probability of
collisions obviously increases which causes longer back-off values of the collided nodes. A suspicious node may be either selfish node (or misbehaving node) which attempts to manipulate its back-off parameters of the CSMA / CA protocol to gain more and more access to the channel, hence get higher performance than their fair share. Suspicious nodes (Misbehavior Node). Which may be an attacker and can increase collisions to decrease the performance of MAC protocols by disobeying CSMA/CA or back-off rules. In this work, we discussed, analyzed and used selfish behavior by attackers to create an opportunistic node. We also identified, declared and finally discard/disassociate the attacker nodes in IEEE 802.11 MAC layer environment. The Access point (AP) Allow most of the nodes offers more bandwidth (in terms of the extra number of slots to almost each node) while maintaining fairness if channel utilization is poor and this mode is called opportunistic mode. The Proposed Protocol is called as the ARA-MAC. The performance of our method is evaluated through a simulation model to test efficiency. Various parameters are the basis for comparison between the implemented method and CSMA/CA. Key Performance Parameters i.e. Packet Delivery Ratio, RTS/Data Frames, Mean no. Of retry per frame have been used for comparison and performance evaluation. The results show that our proposed algorithm ARA-MAC outperforms basic CSMA/CA in terms of Attack Resiliency and Adaptability. ARA-MAC is able to detect and discard attacker nodes after identification of its maliciousness and also it provides adaptability in existing CSMA/CA. The time period for monitoring of node behavior varies according to the Fibonacci series to identify random timing attackers and also it reduces unnecessary execution of ARA-MAC algorithm at AP (Access Point). This is predominantly important in a distributed system where power consumption is a big concern especially in the case of Wireless Sensor Network. It is also important in a centralized system where constant monitoring of a large number of sources from the Access Point (AP) alone may become promptly a big burden on it. The main purpose of this work is to increase the channel utilization by offering opportunities to a node, and detect such node that is using this concept to degrade the network performance in terms of degraded channel utilization.

References

- Seok-Won Kang, Jae-Ryong Cha and Jae-Hyun Kim "A Novel estimation-Based Backoff Algorithm in the IEEE 802.11 Based Wireless Network"; IEEE, CCNC 2010.
ARA-MAC: A Qualifying Approach to improving Attack Resiliency and Adaptability in Medium Access Control Protocol for WLAN 802.11


- Fei Xing, Student Member, IEEE, and Wenye Wang, Member, IEEE, "On the Survivability of Wireless Ad-hoc Networks with Node Misbehaviors and Failures;"
ARA-MAC: A Qualifying Approach to improving Attack Resiliency and Adaptability in Medium Access Control Protocol for WLAN 802.11

Proceedings of the IEEE international Conference on Communications (ICC ’06), 2006.

ARA-MAC: A Qualifying Approach to improving Attack Resiliency and Adaptability in Medium Access Control Protocol for WLAN 802.11

Index Terms
Computer Science
Wireless Communications

Keywords
Attack Resiliency Adaptive MAC Opportunist Mode MAC Misbehavior Selfish Node Attack Contention Window CSMA/CA