A Media Access Control Protocol for Wireless Ad Hoc Networks with Misbehaviour Avoidance

Chaminda Alocious, Hannan Xiao and Bruce Christianson

School of Computer Science, University of Hertfordshire, Hatfield, Herts, UK
{c.alocious,h.xiao,b.christianson}@herts.ac.uk

Abstract. The most common wireless Medium Access Control (MAC) protocol is IEEE 802.11. Currently IEEE 802.11 standard protocol is not resilient for many identified MAC layer attacks, because the protocol is designed without intention for providing security and with the assumption that all the nodes in the wireless network adhere to the protocol. However, nodes may purposefully show misbehaviours at the MAC layer in order to obtain extra bandwidth conserve resources and degrade or disrupt the network performance. This research proposes a secure MAC protocol for MAC layer which has integrated with a novel misbehaviour detection and avoidance mechanism for Mobile Ad Hoc Networks (MANETs). The proposed secure MAC protocol the sender and receiver work collaboratively together to handshakes prior to deciding the back-off values. Common neighbours of the sender and receiver contributes effectively to misbehaviours detection and avoidance process at MAC layer. In addition the proposed solution introduces a new trust distribution model in the network by assuming none of the wireless nodes need to trust each other. The secure MAC protocol also assumes that misbehaving nodes have significant levels of intelligence to avoid the detection.

Keywords: MANETs, Medium Access Control, Misbehaviour Avoidance

1 Introduction

Computer network security is one of the most important elements in computer systems. Wireless networks have been widely used in banking, military, medical and in many other sectors [3]. Wireless network security is becoming increasingly important due to the dramatic enhancement of the wireless devices (e.g. PCs, tablets, mobile phones). There are two types of wireless networks, infrastructure based networks (WLANs) and wireless Mobile Ad-hoc Networks. Infrastructure based networks are controlled by a centralized base station which is the receiver of the network for all the connected nodes [4]. In contrast MANETs are self-organized, dynamically changing the topology without a centralized base station. Wireless nodes in the MANETs communicate by forwarding packets on behalf of each other by working as router.

MANET is an autonomous collection of mobile nodes that communicate over the bandwidth constrained wireless network environment [10] [8]. MANETs need to contain the basic security requirements such as availability, fairness, authorisation, data confidentiality and data integrity [6]. MAC layer nodes misbehaviour has been a problematic scenario for MANETs and infrastructure based networks. Some selfish mobile stations do not follow the IEEE 802.11 protocol rules in sharing medium. IEEE 802.11 protocol assumes nodes in the wireless network fully cooperate to the protocol [10]. However, due to vast enhancement of the programmability of network devices, changing these MAC layer protocol parameters has become easier. Distributed Coordinates Function (DCF) uses the Binary Exponential Back-off (BEB) mechanism to assign back-off for wireless stations, but unfortunately due to vulnerability, this mechanism can be exploited easily. Rest of this paper organized as research background in the next section. Next sections organized as, the proposed secure MAC protocol design and the conclusion.

2 Research Background

The research motivates to provide solutions for following MAC layer selfish misbehaviours.

- **Back-off value Manipulation:** In 802.11 MAC protocol selfish nodes use smaller back-off values than they should and also use fixed back-off values instead of random values. Back-off value Manipulation also includes nodes doesn’t double the congestion window size after a collision.
- **Adaptive Cheating / Adaptive Misbehaviour:** Some nodes are smart to adapt their misbehaviour strategy to prevent them from being caught by regular detection methods. Intelligent nodes are aware of the detection scheme and adapt to mislead the detection.
- **Colluding Nodes:** Sender and receiver can negotiate to misbehave as a pair, in schemes that trusts the sender or receiver or both [6]. Detection of such misbehaviours can be complicated.

MAC layer misbehaviours have been studied from different perspectives using different methodologies. Many researches have focused on solving the MAC layer misbehaviour problems by modifying the existing IEEE 802.11 protocol [1] [2]. These procedures include changing the Binary Exponential Back-off (BEB) algorithm, properties of the CSMA/CA control packets and the authority of back-off value allocation to the receiver [4]. In contrast, statistical inference based detection techniques do not modifying the underlying protocol architecture. Instead these techniques gather the protocol transaction data to analyse misbehaviour [8].

Research done in [4] [5] has identified out many problems, such as receiver misbehaviour, colluding nodes and adaptive misbehaviour. In their approach [4] the receiver assigns back-off value to the sender and monitors the sender’s behaviours. The research carried out by Radosavac et al. in [6] presented their work based on the previous study in [4]. Their protocol has addressed the major drawback in previous proposal in [4] which was assumed the receiver is trusted. Their approach [6] was that sender and receiver agrees through a public discussion on random back-off value. Protocol always ensures that honest party agreed value is truly random. But it is assumed in [6] that one of the parties has to be trustworthy and the honest receiver can monitor the behaviour of the sender and identify the deviation [6]. However, this approach failed to detect colluding nodes. Smart selfish misbehaviour detection method has presented in [9] with a predictable random back off algorithm that can mitigates the effect of the smart MAC layer misbehaviour. Research done by Rong et al. in [8] have explained how statistical and probability models can be utilized to detect cheating stations. This approach has used Bianchi Stochastic Model to build a probability distribution model for packet inter-arrival times.

3 Proposed Secure MAC Protocol and Detection Mechanism

This project aims to propose a secure MAC protocol design, which can be integrated with a novel MAC layer misbehaviour detection and avoidance mechanism. Secure MAC protocol is a novel approach as firstly, the sender and receiver handshake prior to deciding the back-off value but the receiver has the authority to decide the final value. This negotiation requires a mechanism to stop each sender and receiver from generating small back-off values. The secure MAC protocol consists of a statistical analyser as a first line of defence to detect generation of small back-off values. Secondly, secure MAC protocol effectively uses common neighbours to detect misbehaviours at the MAC layer. Common neighbours (CNs) actively work with the sender and receiver in the process of monitoring, detecting and penalizing. In addition the mechanism introduces a new trust distribution in the network by assuming none of the wireless nodes need to trust any other. This trust model is a process of involving CNs to construct a trust distribution to the network. This research also assumes that misbehaving nodes are having significant levels of intelligence to avoid the detection. This research addresses sender misbehaviour, receiver misbehaviour and also colluding node misbehaviour.

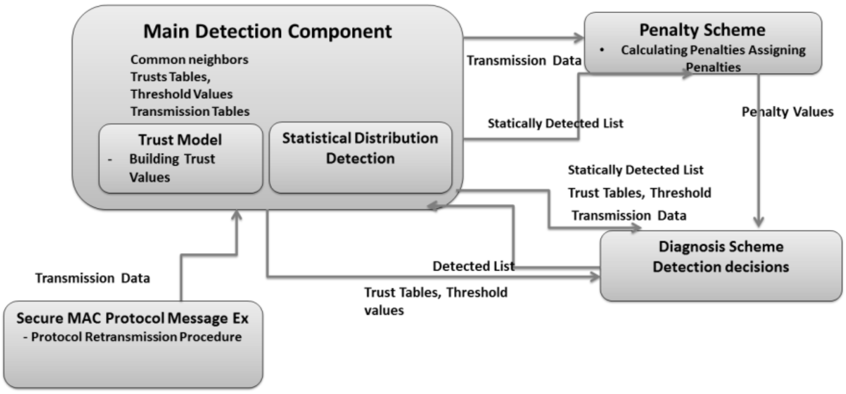

Fig. 1. Secure MAC Protocol and Detection Framework

Fig. 1 demonstrates the proposed Secure MAC protocol. Firstly, the **main detection component** does all the analysis of network traffic and manipulation of CNs data. This main module communicates with other components such as penalty scheme, diagnosis scheme and secure MAC protocol message exchange. This component contains the trust model and statistical data analyser which act as the lowest level of detection technique. Secondly, **penalty scheme** is the module that assigns penalties for deviating senders in each transmission. The third component is **diagnosis module** which performs the detection operation based on the data received by the main detection component, penalty scheme and Trust model.

3.1 Common Neighbours (CNs) and Trust Model

Wireless nodes in the transmission range of both sender and receiver are considered as CNs. The main rational behind using CNs is to build a trust model for the network, monitoring and reporting on node behaviour. For example in **Fig. 2**, nodes 2, 3, 6, and 8 are CNs of nodes 5 and 7. CNs monitoring eliminates most of the unwanted communication overhead. CNs keeps records of the transactions of different sender receiver pairs for a period of time. **Table 1**contains all the transmission details recorded in a neighbour node (node 3 in **Fig. 2**) such as communication ID, expected back-off value (BOV), average sender access times and deviation factor.

According to the Table 1, there are communication entries that were recorded from multiple sender receiver pairs. Ex: Node 3 records communications between sender receiver pairs such as (5-7), (8-7) and (5-3). In **Fig. 2** wireless node 3 records all the transactions of sender receiver pairs of which node 3 is a CN.

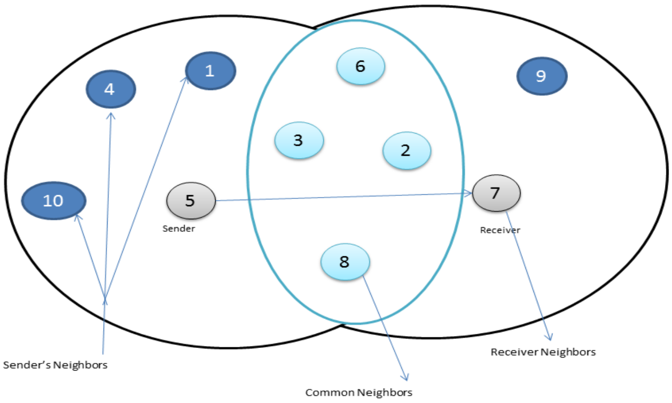

Fig. 2. Distributed Cooperate Detection Mechanism Common Neighbours

Communication ID	Expected BOV	Deviation Factor (∂)	Sender Access
5 → 7	5	4	5
8 → 7	10	4	7
5 → 3	11	10	10

Table 1. Node 3 records during the transmission period

Trust model is the process in which each wireless node builds trust among each other. This trust model assumes that no one has to trust anybody but trustworthiness gradually changes when nodes start to follow the protocol. The trust model is designed in such way that if a node collaborates to detect adversary nodes (observing and reporting) then the node is able to maintain a fair share. Deviation factor represents the selfishness of the given transmission. If the transmission fails to adhere to the expected back-off value then the deviation factor will be increased by 1 if not it will be decreased by 1. The following equation (**Eq. 1**) calculates trust value based on data from **Table: 1**. Node 5 appears twice in the **Table: 1**, let's define that as "**n**" deviation factors (λ) of each of these appearances. The maximum value of (λ) is 10 so each value divided by 10 to get a probability for the node deviation**.** Table: 2 also maintain the nodes status in the network which has defined as normal state (NML) and misbehaving state (MSB).

$$\text{Trust Value (\%)} = \frac{\sum_{k=0}^{n} \lambda_k/10}{n} \tag{1}$$

Node Id	Trust Value (%)	Status
8	50	NML
5	70	MSB

Table 2. Common Neighbour (node 3) Trust value table

3.2 Secure MAC Protocol Message Exchange

The standard IEEE 802.11 protocol message exchange has been modified and re-designed as a security embedded protocol. Provided that DCF control packets such as RTS, CTS, DATA, and ACK been modified to add more data fields. The major inspiration behind modifying the protocol is to change the operation of back-off value calculation and allocation authority, while allowing CNs to be involved in the protocol operations.

3.3 Penalty Scheme (Misbehaviour Avoidance) and Voting Policy(VP)

Penalty scheme is important to discourage wireless node misbehaviours and forces adversary nodes to follow the standard protocol once they have violated it. A penalty value needs to be assigned whenever a node deviates from the protocol. In this proposed protocol, receiver assigns the penalty value to the sender. Voting Policy (VP) is introduced to the penalty scheme to detect colluding neighbours and also to minimize misdiagnosis. VP operates at the receiver end by broadcasting a request to obtain the trust value of the relevant sender in each CN. If sender expected back-off value (B_exp) and the actual back-off value observed by receiver and CNs is B_exp. Following equation (Eq. 2) calculates the penalty value of node id "i". The variable α is a value (0…1) that minimizes the hidden terminal effect in monitoring actual back-off values by the receivers and CNs. Numbers of CNs are defined by "N" and TRV is the trust value of nodes that appear in Table.1. Then the receiver calculates new back-off value by adding penalty to the next transmission.

$$Penalty = (\text{B\_act} - \alpha\text{B\_exp}) * \frac{\sum_{j=1}^{N}(\text{TRVj})}{N} \tag{2}$$

$$\text{NewBackoffValue} = \text{BOV} + Penalty \tag{3}$$

3.4 Diagnosis Mechanism

In this research there are two levels of detection to avoid selfish misbehaviours at MAC Layer. Firstly, detection at random numbers generation level**.** This is a statistical inference detection approach to prevent the nodes to generate small back-off values out of well-known function's distribution. If a node generates such back-off values, then there is a high probability that statistical detection module will name this node as a misbehaving node or increase node's deviation factor. Secondly, detection based on CNs's behaviour monitoring and trust model. After a certain time period and certain number of transmissions the trust values must have saved for each node at each CN, CNs then report their recorded trust values to the diagnosis module for the decision. Diagnosis mechanism calculates the average trust value and makes a decision of node's behaviours.

4 Conclusion

This research has proposed a novel design for a secure MAC layer protocol which is aimed to be resilient for MAC layer misbehaviours. The proposed protocol also assumes that wireless nodes can follow some adaptive misbehaviour strategies to avoid the detection. This research has proposed a novel detection approach which includes the CNs monitoring, trust model and penalty scheme and diagnosis scheme. In the future work, performance of the proposed protocol will be evaluated using ns2 network simulation.

5 References

1. Lolla, V.N., Law, L.K., Krishnamurthy, S.V., Ravishankar, C., Manjunath, D.: Detecting MAC Layer Back-off Timer Violations in Mobile Ad Hoc Networks. In: 26th IEEE International Conference on Distributed Computing Systems, pp.63-63, ICDCS(2006)
2. Jabbehdari, S., Sanandaji, A., Modiri, N.: Evaluating and Mitigating the Effects of Selfish MAC layer Misbehaviour in MANETs. In: IEEE Wireless Communications Letters, vol. 4, 2012
3. Rong, Y.: Detecting Mac Layer Misbehaviour and Rate Adaptation in IEEE 802.11 Networks: Modeling and Sprt Algorithms. In: Ph.D. Dissertation. George Washington Univ., Washington, Choi H., DC, 2008
4. Kyasanur, P.; Vaidya, N.F.: Selfish MAC layer Misbehaviour in Wireless Networks, In: IEEE Transactions on Mobile Computing, vol.4, no.5, pp.502-516, Sept.-Oct. (2005)
5. Gunasekaran, R., Uthariaraj, V.R., Sudharsan, R., Sujitha Priyadarshini, S., Yamini, U.: A distributed mechanism for handling of adaptive/intelligent selfish misbehaviour at mac layer in mobile ad hoc networks. In: Journal of Computer Science and Technology, vol. 24, pp. 472 - 481, 2009
6. Radosavac, S., Cardenas, A. A., Baras, J. S., and Moustakides, G. V.: Detecting IEEE 802.11 MAC layer Misbehaviour in Ad hoc Networks: Robust strategies against individual and colluding attackers. In: Journal of Computer Security, vol. 15(1), pp. 103-128, 2007
7. Rong, Y., Lee, S.K., Choi, H.A.: Overview and Challenges of Routing Protocol and Mac layer in Mobile Ad-hoc Network. In: Journal of Theoretical and Applied Information Technology, 2009
8. Rong, Y., Lee, S.K., Choi, H.A.: Detecting stations cheating on Backoff rules in 802.11 Networks using Sequential Analysis. In: INFOCOM. IEEE, (2006).
9. Guang, L., Assi, C., Benslimane, A.: MAC layer Misbehaviour in Wireless Networks: Challenges and Solutions. In: Journal of Computer Security, vol. 14(4), pp. 6-14, 2008
10. Qin, L., Kunz, T,: Survey on Mobile Ad hoc Network Routing Protocols and Cross-layer Design. In: Carleton University, Systems and Computer Engineering, Technical Report, SCE 04-14, 2004