Computer Communications 55 (2015) 80–101

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Anonymous network coexistence with slotted wireless channel access ☆

Debasmit Banerjee *, Mahmoud Taghizadeh, Subir Biswas

Electrical and Computer Engineering, Michigan State University, United States

ARTICLE INFO

Article history:
Received 3 July 2013
Received in revised form 2 September 2014
Accepted 19 September 2014
Available online 13 October 2014

Keywords:
Network coexistence
Wireless privacy
Traffic analysis
Distributed TDMA
Medium access control

ABSTRACT

This paper presents a novel slotted wireless channel access scheme that preserves privacy across coexisting networks with individual trust domains. The protocol uses a control message free technique and achieves slot allocation without any message-based coordination. Advantages of such a mechanism includes privacy preservation across coexisting networks since there is no explicit interaction among nodes, seamless integration of multiple trust domains without higher layer involvements, and ability to operate in high BER channels. An energy-efficiency module is also designed which uses sleep-wake scheduling to minimize the energy consumption in the system. It was shown that protocols following the proposed mechanism are able to achieve the above goals without any form of time synchronization among the network nodes. We have implemented and evaluated the protocol using NS2 simulator and the performance of the protocol has been demonstrated using extensive simulation models. Energy efficiency has been evaluated by developing analytical models which has been compared with simulation results.

1. Introduction

Wireless ad-hoc and sensor networks are used in emerging applications such as body area sensing, crowd-sensing, intrusion and event monitoring, disaster management, and for a slew of other applications. The advents of embedded wireless technologies in everyday objects have led to proliferation of wireless networks in our daily lives. Due to the open and broadcast nature of the wireless medium, wireless networks are susceptible to passive eavesdropping where an adversary can remain undetected and overhear messages 'flying in the air' to deduce information about the overall network, specific nodes in the network or the relationship between different network nodes. As a result, a critical issue in wireless ad-hoc networks is the threat to the privacy of participating network nodes.

End-to-end encryption mechanisms can prevent the exposure of message content. However, nodes can still be susceptible to linkability [1] wherein an adversary can link multiple sessions from the same user by using node identities exposed in messages. Such linkability can be prevented to some extent by hiding low-level node identifiers using encryption [2,3], or by dynamically modifying the identifiers using pseudonym based mechanisms [4], which can deter user-tracking capabilities of an attacker. These mechanisms, however, require complete coordination and pre-formed trust between coexisting nodes in the network, which may not always be feasible. An adversary can also perform traffic analysis [5,6], which involves the statistical analysis and correlation of identifiable network traffic features, like packet size, frequency of packets, packet inter-arrival times and arrival rate, to deduce communication characteristics and key relationships among nodes. Traffic analysis in a wireless network can lead to user-profiling, link layer topology estimation, user-tracking, and flow-tracking. This can be done even when packets are encrypted and can be used to indirectly identify individual network participants.

For example, a body area network (BAN), composed of wearable sensors mounted or implanted on a person, deal with privacy sensitive patient data which the patient may not want to share with anyone apart from the healthcare provider. The patient may want to stay anonymous during such sensor data collection to prevent any traffic analysis based tracking or profiling by third-parties, advertisers or adversaries. To achieve this, the BAN mounted on one person may use an encryption mechanism such that all sensors on that BAN share a pre-distributed key which is different from that used by the sensors on a different person's BAN. The scenario is explained in Fig. 1(a), in which the nodes in the same BAN trust each other and share information. Then nodes within a BAN is said to belong to the same trust domain, which is a set of mutually trustworthy nodes. When the wireless sensor nodes in two trust domains (i.e. two different BANs) come within communication

☆ This research was partially supported by Grant No. 107784 from the USDA National Institute of Food and Agriculture.

* Corresponding author. Tel.: +1 5173557453.
E-mail address: banerj16@egr.msu.edu (D. Banerjee).

http://dx.doi.org/10.1016/j.comcom.2014.09.010
0140-3664/

range (e.g., Fig. 1(b)), it is necessary for them to coordinate among each other in order to coexist and share the same wireless channel.

Channel sharing using Medium Access Control (MAC) layer coordination such as inter-BAN TDMA slot allocation requires a node to expose its low-layer identifier (i.e., typically MAC address) across nodes outside its own trust domain or BAN. As explained before, exposing MAC address to other trust domains can make the node vulnerable to traffic analysis attacks. Thus the problem at hand boils down to seeking inter-BAN (i.e., inter trust domain) MAC layer slot allocation mechanisms that does not expose any node identity across the BANs. In this paper, we attempt to solve this problem specifically for systems running TDMA MAC.

As another application example, a new internet of thing (IoT) device added to a smart-home system may be from a different vendor which may not be trusted by few other running devices in the home. Such situations may also arise in multi-party disaster rescue operations, privacy preserving crowd sensing applications, and vehicular networks. In general, whenever multiple private wireless networks, running TDMA MAC, attempt to share channel without exposing node identification for preventing traffic analysis attacks, the problem outlined above becomes relevant.

Prevention of node-ID exposure to strengthen unlinkability makes the usage of existing TDMA MAC-scheduling algorithms [7–13] unsuitable. All those scheduling algorithms for distributed wireless networks require the nodes' MAC-layer identities, which are tightly coupled with the network interface, to be shared across trust domains during the TDMA slot scheduling phase. The objective of this work is to develop a distributed TDMA-based MAC scheduling scheme which can allocate transmission slots to nodes belonging to different trust domains. Unlike the existing solutions [7–14], the proposed scheme does not depend on any message-based coordination tactics to achieve TDMA slot assignments, which means that nodes do not need to explicitly share any information during the scheduling phase. To prevent inter-trust domain exposure of data or identity, we assume that entire packets, including the MAC header, are encrypted using an encryption key pre-shared among nodes belonging to the same trust domain. This will prevent any inter- trust domain information leakage during the entire network life-cycle. However, once a MAC schedule is established, nodes within a trust domain (e.g., BAN-1 in Fig. 1) can exchange data by the way of using a trust-domain-specific shared key which is used for opening up the packet at the intended receiver.

The inability to exchange node identity, node location, and transmission schedules introduces new challenges for the design of a distributed TDMA slot-scheduling protocol. To the best of our knowledge, these challenges have not yet been addressed in the literature. In our proposed method, nodes use "blindfolded" packet transmissions where no part of the messages transmitted by one node can be "seen" or deciphered by other nodes from a TDMA MAC scheduling standpoint. This introduces a zero exposure environment. Nodes can only "hear" the presence of messages through listening to the channel. The proposed protocol uses such "blindfolded" listening to infer timing of transmitted packets and a novel pattern-based shadow packet mechanism for two-hop TDMA slot information dissemination.

These two key innovative concepts are used to design a distributed TDMA slot self-scheduling algorithm which relies only on local information at nodes and does not require any network time synchronization. Such a mechanism can enable coexistence between nodes belonging to different TDMA based private networks for which traffic analysis is a concern. Furthermore, since all nodes in a TDMA network send packets with the same periodicity, it is naturally more difficult [15,16] for an adversary to perform traffic analysis as it does not provide a direct correlation between extractable traffic features, like frequency of packets, packet inter-arrival times, arrival rate, and delay characteristics. Also, since the primary theme of the protocol is to work without any packet decoding, further advantages include seamless addition of new network participants without revealing any information about the existing network participants, as well as reduced impact of high-error channels on the slot allocation process. Since the transmission scheduling is independent of any message-based information, a low SNR would have lesser impact than mechanisms which depend on explicit control messages. Additionally, nodes that are within the carrier sensing range but not within direct communication range can also coordinate to allocate collision free slots, resulting in a sooner onset of the convergence process than possible with control message-based schemes.

The contributions of the paper are as follows. First, we develop ZEATDMA, which uses time-coded packet transmissions and pattern-based shadow packet mechanism for MAC slot scheduling. The main concepts of this protocol have been presented in our prior work [17]. In this paper, we present a steady state energy efficiency module which can be used on top of the baseline ZEATDMA. Additionally, an analytical model for the steady state energy consumption is developed for better understanding of the energy consumption when the energy efficiency module is used. We simulate the energy consumption during steady state and compare it with the analytical results to validate our model. We also present ZEATDMA-NS, which is a simpler version of the ZEATDMA. It is shown that when energy-efficiency is not a priority, ZEATDMA-NS can accomplish anonymous MAC slot allocation with significantly less complexity compared to the baseline ZEATDMA. Finally, through extensive NS2 simulations, both ZEATDMA and ZEATDMA-NS are functionally validated and their performances are evaluated under varying topology and network dynamics. Simulation results showing the energy consumption during the slot allocation process have also been presented to demonstrate the overhead (or the lack thereof) of the scheduling process.

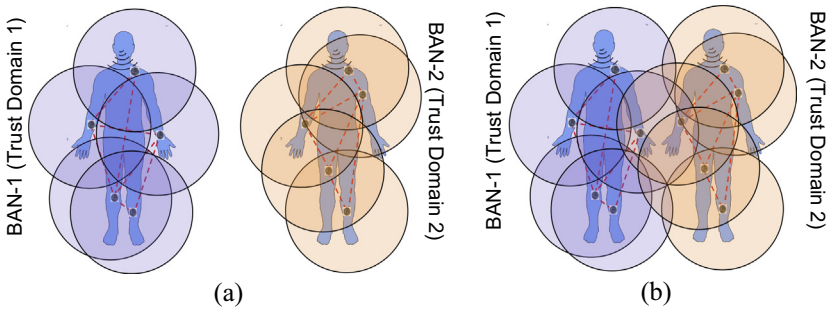

Fig. 1. Trust domains and channel sharing across body area network (BAN).