A Security Protocol in UWB and WiFi Networks

WU Huayi [1], BAI Baohua [2]

[1] School of Automation & Electrical Engineering University of Science and Technology Beijing, Beijing 100083, China
[2] Communication & Power Utilization Technology Subcompany State Grid Electric Power Research Institute, Beijing 102200, China
wuhuayi@ustb.edu.cn

Abstract - In this paper, we studied a hybrid wireless network including UWB devices and WiFi devices together and analyze the characteristics of selfish behavior and the methods how to expose it. In order to improve the self-giving cooperation between the nodes in hybrid wireless networks and increase the fairness index of the whole networks, a security mechanism was proposed in this paper. The punishment mechanism was used both in a common control channel and a data channel. The results of stimulations show that the proposed protocol improves the self-giving cooperation between nodes in the networks and make the interference of the network minimum.

Index Terms - security protocol, UWB, WiFi, interference

1. Introduction

With the increase of demands for higher-rate wireless communications, an advanced communication technology called ultra wideband (UWB) attracts much attention lately. UWB is characterized as a signaling technique with ultra-wide signal bandwidth and reduced power spectral density, which was allowed by FCC (Federal Communications Commission) as regulation for commercial use in 2002 [1].

ECMA Standard 368 [2] specifies the ultra-wideband (UWB) physical layer (PHY) and medium access control (MAC) sublayer for a high-speed short range wireless network, utilizing all or part of the spectrum between 3 100 - 10 600 MHz supporting data rates of up to 480Mb/s. Due to the properties large spectrum and short transmission rang (no more than 10m), the immediate application of UWB is thought to be in the WPAN (Wireless Personal Area Network) space, such as for home networks or cable replacement around a personal computer [3]. WiFi[4] allows cheaper deployment of local area networks (LANs). Thus in an indoor wireless environment including UWB devices and WiFi devices together, how to control the interference of the network to improve the network throughput become new noticeable issues. In this paper, a new scheme is proposed to decrease the interference of the network. Therefore, the network throughput is improved.

Selfish Behavior is a kind of widespread attacks of MAC layer in wireless networks [5] [6]. Selfish behavior attack refers that the normal equipments in the network improve their own communication by launching a series of the abnormal behaviors to weaken the overall performance. In IEEE 802.11 DCF, selfish nodes unilaterally amend the fallback mechanism to obtain access to the parameters of the priority of the channel and cause selfish nodes to achieve better throughput.

The rest of the paper is organized as follows. Related work is presented in the next section. Section 3 describes problem. Section 4 analyses the proposed security protocol. Simulation results and analysis are discussed in the Section 5 and finally, the paper is concluded.

2. Related Works

A. Protocol in a hybrid wireless network

The Ultra-wideband (UWB) is an emerging technology designed for short range and high transmission rate [7], [8] and [9]. Related works can be classified into two categories. The first category is to construct topology in structured MAC, such as [10]. Some studies for relay node placement are introduced in [11], [12] and [13] although they focus on sensor networks. The second category is to study the interference and calculate achievable throughput in multihop UWB networks, such as [14], [15], [16]. Radunovic et al. [16] jointly considered power control, scheduling, and routing in UWB networks, to optimize the throughput.

Different from the above schemes, the scheme proposed in this paper considers both network planning and topology control in order to reduce the expense of network planning and decrease the interference of the network.

B. Security mechanism in wireless networks

In general, the solution of selfish behavior mainly includes three types, incentives, penalties and game. IEEE802.22 draft [17] [18] did not consider the selfish behavior in cognitive radio networks. In [19], authors put forward a sub-cluster program to solve cognitive radio networks in the selfish behavior from a routing of view. In IEEE 802.11 DCF, selfish nodes unilaterally amend the fallback mechanism to obtain access to the parameters of the priority of the channel and cause selfish nodes to achieve better throughput. Kyasanur and Vaidya in [20] proposed a MAC selfishness hindering detection program and correction mechanism. Their main idea was to allow the recipient to distribute and send back value in the CTS and ACK frames, and then to use the values to detect the misbehaviors. The correction program is that if selfish behavior is detected, punishment will be executed at the next back time. Cagalj in [21] used a game-theoretic frame to study the selfish behavior of MAC layer. Through a dynamic game model, he got a more balanced strategy for the network. In the model, each node controls its own channel access probability by adjusting its own contention window. This model is effective when all nodes are within the scope of their respective transmission.

3. Problem Formulation

Our problem is to find a security routing protocol in order that each UWB or WiFi device indoor can connect the gateway (Internet) directly or indirectly by relays of other devices which can be other UWB or WiFi devices indoor or other UWB or WiFi relay devices newly added to the network.

If there are margins in the network, that is to say, there are some UWB or WiFi devices indoor which cannot connect the gateway no matter directly or indirectly if no new UWB or WiFi relay device is added to the network, we need to find a minimal Steiner tree whose Steiner nodes are minimal and whose cost is minimal. The cost of a tree is the sum of interference of the whole links of the tree. Because Steiner Minimum Tree with Minimum number of Steiner Points (SMT-MSP) problem is NP- hard [22], we propose a strategy MRN to solve the problem. The followings are some simple steps of MRN. The detailed algorithm will be given in the next section.

Step1: to adjust the power level of all the UWB or WiFi devices indoor to the maximum.

Step2: to add some new UWB or WiFi relay devices to the margin zones in order that the network indoor is connected. At the same time, to minimize the number of the new UWB or WiFi relay devices. That is to say, to find a minimal Steiner tree with minimal Steiner nodes.

Step3: to adjust the power levels of all the UWB or WiFi devices indoor and those new UWB or WiFi relay devices in order to minimize the interference of the network and increase the network throughput under the condition that the network is connected.

4. Security Mechanism Design

The proposed improved security mechanism considers the punishment to selfish nodes both in a common control channel and a data channel for UWB nodes or WiFi nodes.

When a new node A joins a network, it will broadcast a request frame NEWN_req in control channel firstly. NEWN_req includes A's own identity crIDA, the range of channel that A can sense ch_{num}, and channel No. that A senses chID:

$$A \to *: NEWN\_req(crID_A, ch_{num}, ch_{ID});$$

When node B receives the request, it will return a sensing feedback SEN_rep, including its identity crIDB, the number of channels it senses ch_{num}, and the channel No. it senses chID:

$$B \to A: SEN\_rep(crID_B, ch_{num}, ch_{ID}).$$

A saves the message SEN_rep that comes from B and maintains a table called Neighbor Nodes Sensing Ability List(NNSAL), which records the sensing capability of each node. It includes table sequence (TS) S_i, node identity (NI) n_i, the number of channels that node sensed (NCNS) N_i, the channel No. that node sensed (CNNS) and selfish index of each node (SI) v_i. The initial value of v is 0.

Suppose that the number of channels available across the network is m and the number of nodes is n, so the range that a node can sense is $m/n < N_i \le m/n + a$, $a \in N$.

The ratio between k and v is $k/v = 8$, if the value of k increased by 1, then $k = v*8$, Which $0 \le v \le 32$, $0 \le k \le 128$.

The proposed punishment mechanism is designed as follows:

Step 1: When the node S requests to send data to node R, send its own $FCL_S = (ch_{s1}, ch_{s2} \cdots\cdots ch_{sn})$ to node R.

Step 2: Once R receives FCLS, it compares FCLS with the NNSAL that it keeps firstly. If there are some new channels in FCLS that aren't kept in NNSAL, then there may be the existence of selfish behavior of S.

R won't send SEL frame to S. R create a random number RR, increase the SI v_S by 1, then decide a k according to v_S.

Step 3: then R broadcast the information including crIDs, RR, k and a timestamp TR.

$$R \to *: (crID_S, R_R, k, T_R),$$

Once other node n_i receives the message, it will know that S is a selfish node, and R is ready to send a puzzle to S. It increases S's v_S in its own NNSAL by 1, saves RR, and stops every request from S.

Step 4: Once S get the message, S has to break the puzzle to continue the communication with other nodes. It creates a random number RC, and then tries to break the puzzle for the solution X with its own identity crIDs in the hash function below:

$$h(crID_S, R_R, R_C, X) = 0_1 0_2 ... 0_k Y$$

Step 5: Once S breaks the puzzle, it will broadcast the solution X as follows:

$$S \to *: (crID_S, crID_R, R_R, R_C, X)$$

Step 6: Other node n_i will know that S has broken the puzzle and waiting for the verification from R.

Step 7: R verify the solution X with the function $h(crID_S, R_R, R_C, X) = 0_1 0_2 ... 0_k Y$, if X is the right solution, R broadcasts a signature message RE_use as follows to tell other nodes that S has broken the puzzle, the stopped communication can be restarted.

$$R \to *: K_R^- (crID_S, RE\_use, T_R)$$

Then R send a SEL to continue the communication stopped before, other node n_i will reponse request from S after receives RE_use.

In the ensuing period of time T, other nodes will be listening for perception of the region S and broadcast the results that they sensed. S reports its sensing results to the entire networks. Other nodes compare the sensing information they sensed to the information that S reported. If S reports its sensing information honestly v_S will be decreased by 1,

otherwise v_S will be increased by 1. In order to avoid breaking a puzzle with a lot of time and resource consuming, S has to maintain its record in others' NNSAL at an acceptable value, so it has to disclosure the information that it has sensed honestly. When k > 64 calculations for elapsed time will be very large; when k = 128, break the puzzle will be not feasible in the calculation. When v reaches an unacceptable value selfish nodes have to consider withdrawing from the network and re-send the application to join the network.

5. Simulations

$$\text{Fairness index} = \frac{\left(\sum_f R_f\right)^2}{n\sum_f R_f^2} \quad (1)$$

where R_f is the measured throughput of each data flow and n is the total number of flows in a given network.

This paper uses the NS-2.31 to simulate the performance of our proposed mechanism SC-MAC, test the fairness of selfish behavior on the network impact in UWB and WiFi networks and the effect of our proposed Security Protocol with Minimum Interference (PMSP). The Scenario range is 1000m×1000m, the channel capacity is 480Mb/s and 100Mb/s with CBR data stream and TCP as transport protocol. Each UWB node has 30 channels and its transmission range is 10m. There are 100 nodes in all, 60 for normal nodes while 40 for selfish nodes. If selfish nodes are rarely selected as the data forwarding node in the edge of the region, they don't affect the fairness of the entire network very much, so selfish nodes are deployed in the network core area.

We stimulate the following situation. Selfish nodes send false information control channel frame based on Poisson process. Then compare PMSP with PBPM in [24] by the same scene. With three sets of simulation results we get network throughput data and calculate function (1). The results are shown as Fig.1.

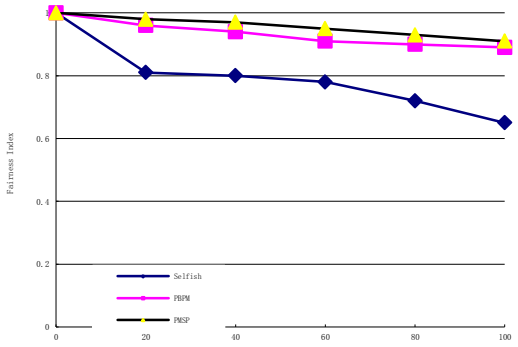

Fig. 1. The Impact to Fairness Index

We conducted three sets of simulation experiments. The simulation results from figure 1 we can see, a fair index of the network without PMSP or PBPM gradually decreased with the increase of the proportion of selfish nodes eventually stabilized at around 0.7. In the second group of simulation, the 60 normal nodes run PBPM and then run PMSP in the third group of simulation. From the simulation results we can see, the hybrid network which is running PMSP has a more stable throughput. Its fairness index has not been impacted by the number of selfish nodes. When all selfish nodes began to work, FI remained stable throughout the network and no dramatic decline. We can see that PMSP improves the FI of the entire network. PMSP makes nodes cooperate selflessly.

Acknowledgment

This work is supported by the Fundamental Research Funds for the Central Universities (No. FRF-TP-12-098A), and National Natural Science Foundation of China (No. 61240008).

References

[1] Federal Communications Commission, "Revision of Part 15 of the Commission's rules regarding Ultra-Wideband transmission systems," FCC 02-08, Apr. 2002.

[2] ECMA-368, "High Rate Ultra Wideband PHY and MAC Standard," December 2005.

[3] G. Kim, A. Rajeswaran and R. Negi, "UWB versus 802.11 - a network. Perspective, "Broadnets 2006, CA. USA.,Oct. 2006.

[4] Wi-Fi Alliance: White Papers. http://www.wi-fi.org/wp/wifi-alliance-certification/. Retrieved 2009-10-22.

[5] K. Bian, J. Park. "MAC-Layer Misbehaviors in Multi-Hop Cognitive Radio Networks," Proc. 2006 US-Korea Conference on Science, Technology, and Entrepreneurship(UKC2006), pp.1–8.

[6] L. Zhu, H. Zhou, "Two Types of Attacks against Cognitive Radio Network MAC Protocols," Proc. 2008 International Conference on Computer Science and Software Engineering, 2008, pp.1110–1113.

[7] Xuejing Wang, Liang Liu, Fan Ye, Junyan Ren, Bo Hu, "A Novel Synchronizer for OFDM-based UWB System on New Preamble Design", the 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'07), Greece, 2007, pp. 1-5.

[8] A. F. Molisch, "Ultrawideband propagation channels and their impact on system design," 2007 International Symposium on Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications, Aug. 2007, Hangzhou, pp. K4- 1-K4- 5.

[9] D. Cassioli, R. Giuliano and F. Mazzenga, "Performance evaluation of high data rate UWB systems based on IEEE 802.15.3", 2005 IEEE International Conference on Ultra-Wideband, Sept. 2005, pp.678- 683.

[10] Q. Wu, Y. Xiong, Q. Zhang, Z. Guo, X. Xia, Z. Li, "Joint routing and topology formation in multihop UWB networks, "IEEE Journal on Selected Areas in Communications, April 2006, volume 24, issue 4, part 1, pp. 843- 849.

[11] B. Hao, J. Tang and G. Xue, "Fault-tolerant relay node placement in wireless sensor networks: formulation and approximation", IEEE Workshop on High Performance Switching and Routing (HPSR'2004), pp. 246-250.

[12] X. Cheng, D.Z. Du, L. Wang and B. Xu, "Relay sensor placement in wireless sensor networks", ACM/Springer Journal of Wireless Networks, accepted for publication, available at http://www.seas.gwu.edu/~cheng/Publication/relay.pdf.

[13] D. Chen, D. Du, X. Hu, G. Lin, L. Wang, and G. Xue, "Approximations for Steiner trees with minimum number of Steiner points," Theor. Comput. Sci. 262, 1-2, Jul. 2001, pp. 83-99. DOI= http://dx.doi.org/10.1016/S0304-3975(00)00182-1.

[14] Y. Zeng, N. Han, S.- H. Sohn, J.-M. Kim, "Hybrid UWB Multi-Piconet Network Interference Modeling and Performance Enhancement by 6-

Bands MB-OFDM", The 9th International Conference on Advanced Communication Technology, 2007, vol. 1, pp. 839 – 843.

[15] B. Radunovic and J.-Y. Le Boudec, "Optimal power control, scheduling, and routing in UWB networks," IEEE Journal on Selected Areas in Communications, Sep. 2004, vol. 22, pp. 1252–1270.

[16] M. Burkhart, P. von Rickenbach, R. Wattenhofer, A. Zollinger, "Does Topology Control Reduce Interference?", *MobiHoc'04*, May 2004, Roppongi, Japan, 2004, pp. 9-19.

[17] IEEE 802.22 working group on wireless regional area networks. http://www.ieee802.org/22/.

[18] IEEE 802.22/D0.1, Draft Standard for Wireless Regional Area Networks Part22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Policies and procedures for operation in the TV Bands, IEEE Standard , 2006, pp. 235–247.

[19] N. Xue, X. Zhou, T. Liu, X. Xin. "Cluster-based Security Architecture for Distributed Cognitive Radio Networks," Telecommunications Science, 2008, 52–56.

[20] P. Kyasanur and N. Vaidya, "Selfish MAC Layer Misbehavior in Wireless Networks," IEEE Transactions on Mobile Computing, vol. 4(5), 2005, pp. 502–516.

[21] M. Cagalj, S. Ganeriwal, I. Aad, and J.-P. Hubaux, "On selfish behavior in CSMA/CA networks," Proc. IEEE INFOCOM, vol. 4, 2005, pp. 2513–2524.

[22] G. Lin and G. Xue, "Steiner tree problem with minimum number of Steiner points and bounded edge-length," *Information Processing Letters*, vol.69, 1999, pp.53-57.

[23] R. Jain, The Art of Computer System Performance Analysis. John Wiley and Sons, Inc. 1991.

[24] H. Wu, N. Hui, X. Zhou and B. Bai, "Puzzle-based Selfish Behavior Punishment Mechanism of MAC Layer in Cognitive Radio Networks," Proc. the IET 3rd International Conference on Wireless, Mobile and Multimedia Networks (ICWMMN 2010), IET Press, Sep. 2010, pp.213–216.

[25] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," *IEEE Translated J. Magn. Japan*, vol. 2, pp. 740-741, August 1987 [*Digest 9th Annual Conf. Magnetics Japan*, p. 301, 1982].

[26] M. Young, *The Technical Writer's Handbook*, Mill Valley, CA: University Science, 1989.