ZESZYTY NAUKOWE AKADEMII MARYNARKI WOJENNEJ
SCIENTIFIC JOURNAL OF POLISH NAVAL ACADEMY

2015 (LVI) 4 (203)

DOI: 10.5604/0860889X.1187607

Andrzej Marczak*

THE SECURE TRANSMISSION PROTOCOL OF SENSOR AD HOC NETWORK

ABSTRACT

The paper presents a secure protocol of radio Ad Hoc sensor network. This network operates based on TDMA multiple access method. Transmission rate on the radio channel is 57.6 kbps. The paper presents the construction of frames, types of packets and procedures for the authentication, assignment of time slots available to the node, releasing assigned slots and slots assignment conflict detection.

Key words:
Ad Hoc, ASAP, OFB Mode, TDMA.

INTRODUCTION

The Time Division Multiple Access (TDMA) method is often used in Ad Hoc sensor networks because of its ability to ensure collision-free transmission of packets regardless of the amount of traffic on the network. Many types of transmission scheduling protocols are used in TDMA Ad Hoc networks. Some of them do not support autonomous behaviors of mobile nodes. They cannot update the slot assignment of each node due to arrival or exit of mobile node [2]. Unifying the Slot Assignment Protocol (USAP) [4] and USAP-MA [5] Protocol, allows the operation of networks whose topology dynamically changes.

However, they are characterized by poor channel utilization because of the existence of many conflicting or unassigned slots.

* Gdańsk University of Technology, Faculty of Electronics, Telecommunications and Informatics, G. Narutowicza 11/12 Str., 80-233 Gdańsk, Poland; e-mail: amarczak@eti.pg.gda.pl

The sensor Ad Hoc network protocol, presented in this paper, uses the TDMA method and the Adaptive Slot Assignment Protocol (ASAP) protocol [1]. The ASAP protocol was chosen because of its ease of implementation in hardware and good properties [1]. This protocol is enhanced with authentication and encryption procedures.

TDMA FRAMES STRUCTURE

A sensor network consists of Server, Personal Identification Module nodes (PIM) and Reference Node nodes (RN) (fig. 1). The hierarchy level of RN indicates the number of radio hops to the server. Hierarchy level 0 means that the RN is connected via a wired connection to the server. Network nodes transmit seven types of packets:

- data packet — DATA;
- request packet — REQ;
- information packet — INF;
- hierarchy level packet — LEVEL;
- suggestion packet — SUG;
- reply packet — REP;
- authentication packet — AUTH.

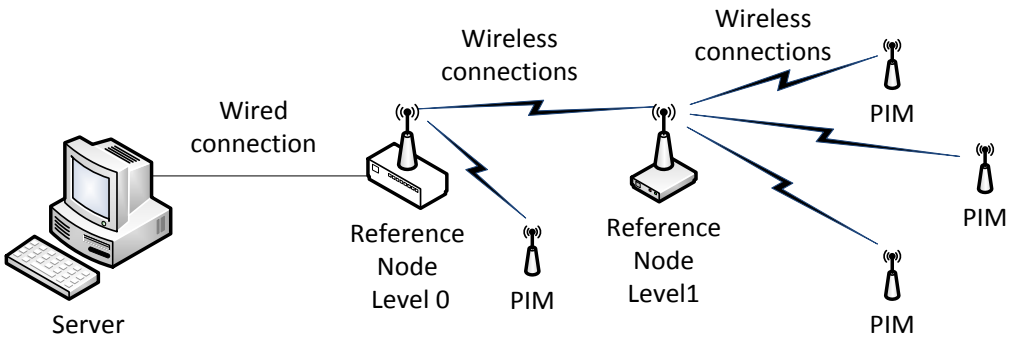

Fig. 1. Secure sensor network

Packets are transmitted in the frames. The frames are organized into superframes. The primary (shortest length) superframe has 4 time slots. The duration of the superframe is 20 ms. The ASAP protocol allows the use of long superframes. The lengths

of such the superframes are multiples of the primary superframe. The length of the long superframe is set as a power of two. The superframes can be composed of 8, 16, 32 and 64 time slots, respectively. Such superframe durations will be then of 40 ms, 80 ms, 160 ms and 320 ms.

Transmission rate at the radio interface is 57.6 kbps, so the duration of the 1 bit is t_b = 17.36 μs, and the duration of 1 byte is t_B = 8 x t_b = 138.88 μs. The duration of the 33-byte data packet (DATA) t_r = 4.583 ms. The duration of the time slot t_s = 5 ms, so guard intervals have 2 x 208.48 ms (416.96 μs), or duration of 3 bytes. In the case of packet types with fewer bytes, we used the addition of appropriate number of zero bytes (0 x 00) to align the packet length.

Figure 2 shows the frame and superframe in a sensor network. The first slot in the superframe (ZPS) has been reserved for the new node to transmit control Request packets (REQ) or authentication packet (AUTH).

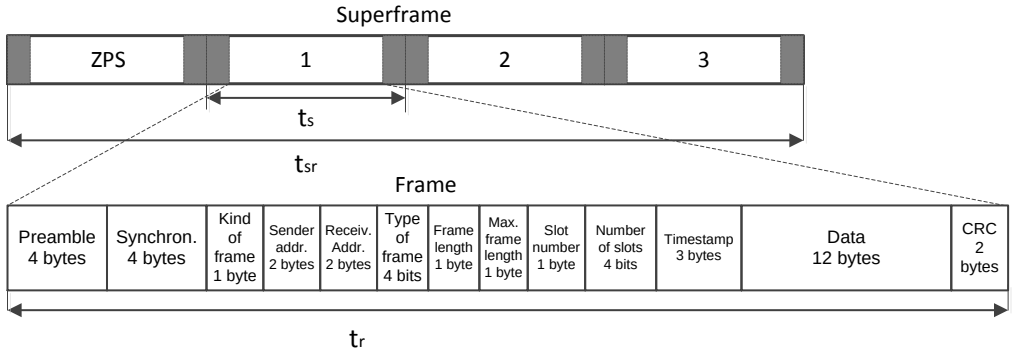

Fig. 2. Frame and superframe in secure sensor network

This way, no data packets (DATA) are transmitted in this time slot. The data packets can be transmitted over the remaining three time slots (for the superframe with length L = 4). The same is true in the case of superframes with a greater number of time slots. The first time slot is always ZPS, used for the REQ or AUTH packets to be transmitted, and the remaining slots are used for data transmission.

Each packet type has a fixed part depending on the structure of the packets sent by used the radio modems. This fixed part has a 4 byte preamble, 4-byte synchronization and 1 byte the kind of frame information. The PIM node addresses will have values between 0 (0 x 00) to 127 (0 x 7F), while RN will have address values from 128 (0 x 80) to 254 (0 x FE). Address with a value 255 (0 x FF) is for a broadcast transmission. In the case of transmission towards the server in packet address

fields will be the source address (PIM or RN) and the address of the next RN node (the destination node). The RN node receiving the packet containing its address as the target, it checks its routing table to the next RN node address in the direction of the server and forwards the received packet in a different time slot. In the case of transmission from the server, the source address is the address of RN node sending the packet and the destination address is the address PIM or RN node (if the packet is sent to the RN node).

PACKET FORMATS

Transmit mode

The data packet (DATA) (0 x 0D) is the first type of packets. It contains information on the frame length and time slots assigned to the sender, and the maximum frame length of the sender and its neighbors [1]. This packet also contains the encrypted data sent by a node.

Control mode

1. Request packet (REQ) (0 x 0C) is transmitted by only a new node. By sending this packet to neighbors, a new node requests the information on the frame length and assigned time slots of all nodes in contention area [1].
2. Information packet (INF) (0 x 0B) contains the information on the frame length of the sender and time slot assigned to the sender and its neighbors [1].
3. Hierarchy level packet (LEVEL) (0 x 6) is transmitted periodically by a RN node in the ZPS time slot. The RN node is sending the packet to its neighbors, informing all nodes about its network hierarchy level.
4. Suggestion packet (SUG) (0 x 0A) is transmitted by only a new node. By sending this packet to the neighbors, the new node announces the frame length and its assigned slot [1].
5. Reply packet (REP) (0 x 05) is transmitted for the confirmation of receiving SUG packet [1].
6. Authentication packet (AUTH) (0 x 01) is used in the authentication procedure. This packet sends an encrypted node address and the encrypted session key (in 2 consecutive packets).

DATA SECURITY

The security of the transmission is ensured by the use of the block cipher algorithm (e.g. AES, 3DES) working in Output Feedback (OFB) mode (fig. 3). The OFB mode uses the initialization vector IV. In this solution IV vector is a timestamp. Its uniqueness is critical. The ciphertext is obtained by the modulo 2 addition of the plaintext bits (P) and block cipher output bits (O). Block cipher output bits only depend on the cipher algorithm, session key K and initialization vector IV (timestamp) [3]. One advantage of the OFB mode is low sensitivity to transmission errors, and more specifically the lack of error propagation [3]. Using the OFB mode we can encrypt data blocks of any length, even shorter than the length of the data block used in encryption algorithm (e.g. 128 bits in AES algorithm).

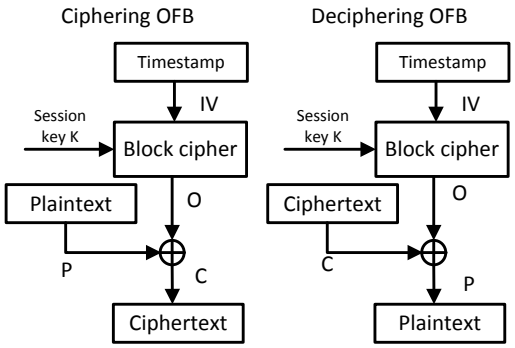

Fig. 3. Ciphering and deciphering in sensor network

AUTHENTICATION PROCEDURE

The OFB mode is used in the procedure of authentication nodes (PIM, RN), and to encrypt data transmitted in the DATA frames. The authentication procedure takes place after the new node determines the first time slot (ZPS) in the super-frame. All network nodes keep in the memory a pair of numbers (8-bit address) and the master key (128 bits)). The same pair of numbers is stored in the server, which acts as a Key Distribution Center (KDC). Only node whose data (address and master key) are stored in the memory server can connect to the network. Authentication is performed after the connection to the KDC server. The transmission associated with the authentication is performed in the ZPS time slot. The s slot assignment procedure to the new node occurs only after successful authentication. The result of

authentication procedure is to provide the RN or PIM the session key K, which is necessary for the exchange of information with the server. The session key is the same for all nodes in the network. Its validity can range from a few to several hours. The length of the session key depends on the encryption algorithm. For the AES algorithm key length is equal 128 bits. The authentication procedure consists of four steps:

1. The node that wants to connect to the network transmits in ZPS time slot, authentication packet (AUTH) containing his encrypted address. The address is encrypted using a master key.
2. The server, based on the node address, searches in its memory the master key and decrypts the encrypted address. Then, it compares the two addresses (the decrypted address and the address sent without encryption in the address field of the frame).
3. If the comparison result is positive, the server encrypts 128-bit session key K using the master key and sends it to the authenticated node also in the ZPS time slot. Negative comparison result ends the authentication procedure. The server sends one AUTH packet containing zero.
4. The node receives the encrypted session key K and decrypts it. Since then, all transmitted data is secured. From that moment, the entire transmission is secure. In the case of a negative authentication, after receiving the AUTH packet with the content zero, the node, after a few superframes, may initiate a re-authentication procedure.

TIME SLOT ASSIGNMENT PROCEDURE

The time slot assignment procedure is performed after successful authentication of the new node. All RN nodes, passing AUTH packet with a message about the negative authentication (1 packet containing zero — 8 bytes of 0 x 00) know that the node is unauthenticated and cannot compete for access to the channel. After successful authentication the new node selects a time slot assigned to itself in four steps.

Requesting the information on time slot assignment in the contention area

When a new node joins the network, it does not know the information on network topology or time slots assigned to other nodes in its contention area. To get this information, the new node listens to the channel and checks packets transmitted from the neighbors. DATA packets from neighbors contain the information on their

assigned slots, superframe length, and maximum superframe length. From these pieces of information, the new node knows the position of the first time slot in a superframe and maximum superframe length among all nodes in its contention area. Then the new node sends a REQ packet (0 x 0 C) in the first time slot of the next superframe. Neighbors that have received the REQ packet transmitted from the new node, transit to the control mode. Each neighbor of the new node gives information in its superframe length and time slot assigned to itself and its neighbors by transmitting an INF packet (0 x 0 B) in its assigned time slot. After all neighbors of the new node have transmitted INF packets, all nodes in the contention area of the new node can know its structure [1].

Setting the superframe length and time slot assignment

After receiving INF packets from all neighbors, the new node sets its superframe length. If all nodes in its contention area have the same superframe length, the new node sets its own superframe length to this length. Otherwise, the new node uses the maximum superframe length among all nodes in the contention area. Then, from received INF packets, the new node knows the information on slot assignment in this contention area. The new node creates its own time slot assignment information of superframe length, S_0 where S_0 denotes the frame length that is set to the new node. If the superframe length of a neighbor is same as S_0, the time slot assignment information of the neighbor is copied to that of the new node. Otherwise, if $S_0 = a \cdot S_i$, the time slot assignment information of the neighbor is copied repeatedly to every S_0/a slots. S_i is the superframe length of the neighbor and a is an integer of a power of two. The new node merges the information from all neighbors and creates its own time slot assignment information [1].

For example, when the new node sets its superframe length as 8, the time slot assignment information in the INF packet received from node b whose superframe length is 4 and assigned slot is 2 is copied repeatedly to every 4 time slots in that of the new node (fig. 4) [1].

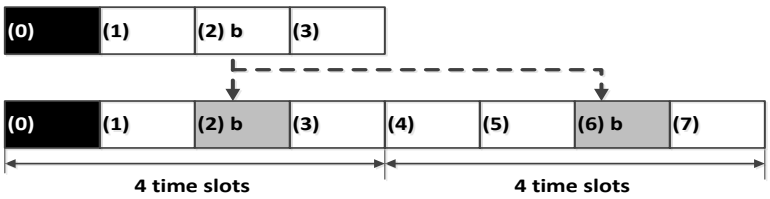

Fig. 4. Copying information about node *b* [1]

Selecting an assigned time slot

Based on the time slot assignment information, the new node selects a time slot assigned to itself by three procedures:

- Getting an unassigned slot (GU) [1].

If some unassigned time slots are found in the time slot assignment information, the new node assigns one of them to itself. For example when unassigned time slots 3 and 7 are found, the new node can assign a time slot either 3 or 7 to itself (fig. 5) [1].

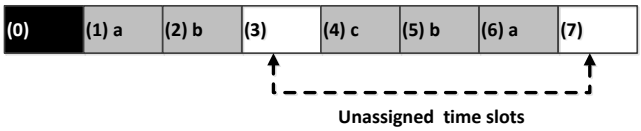

Fig. 5. Getting unassigned time slots [1]

- Releasing multiple assigned time slots (RMA) [1].

If no unassigned time slot is found, the new node checks whether some nodes in the contention area are assigned multiple time slots. If such node is found, the new node releases one of these time slots and assigns it to itself. If there are more than one node to which multiple time slots are assigned, the node with the largest number of assigned time slots among them is chosen to release a time slot [1]. For example, when node *a* and *c* are assigned multiple time slots, the new node selects a time slot from time slots 1, 3, 6 and 7 which are assigned to nodes *a* and *c*, and assigns the selected time slot to itself (fig. 6) [1].

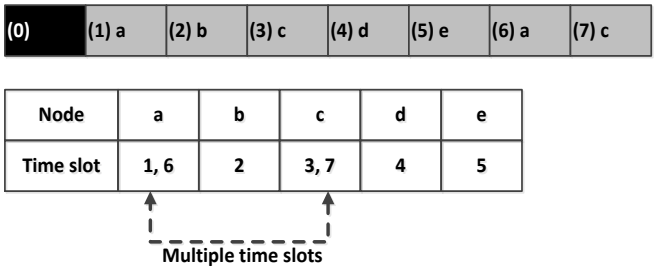

Fig. 6. Releasing multiple assigned time slots [1]

- Doubling the frame (DF) [1].

If no unassigned time slot is found and no node has multiple assigned slots which are able to be assigned to the new node, the new node doubles the superframe

length of the slot assignment information and copies the assignment information to both of the former half and the latter half of doubled superframe. The first time slot in the superframe is not assigned to any nodes. Therefore after doubling the superframe length, the first time slot in the latter half becomes unassigned slot. The new node assigns this time slot to itself [1]. For example when the new node doubles the superframe length, slot 8 can be assigned to itself (fig. 7) [1].

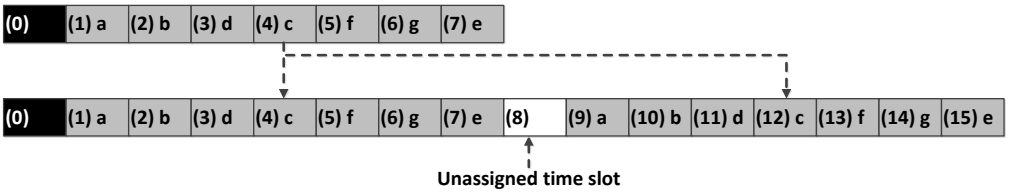

Fig. 7. Doubling the superframe [1]

Announcement of updating the time slot assignment information

After selecting a time slot assignment, the new node in network sends a SUG packet to its neighbors. The SUG packet contains information on the superframe length and the assigned time slot. When the neighboring nodes receive this packet, they update time slot assignment information. After updating the information based on the received SUG packet, each neighboring node sends a REP packet to its neighboring nodes. Sending this packet implies the confirmation of the SUG packet for the new node and announcement of updating the time slot assignment information and exiting from the control mode. The sender and receivers of the REP packet adopt the new time slot assignment and can restart data transmission from the next superframe. The new node, after receiving the REP packets from all neighboring nodes, transits to the transmit mode [1].

DETECTION OF CONFLICT

In the protocol, a conflict of slot assignment occurs when a new node connects to two or more nodes to which the same time slots are assigned. In the example (fig. 8), a conflict occurs at a new node between node *c* and node *f* in time slot 5.

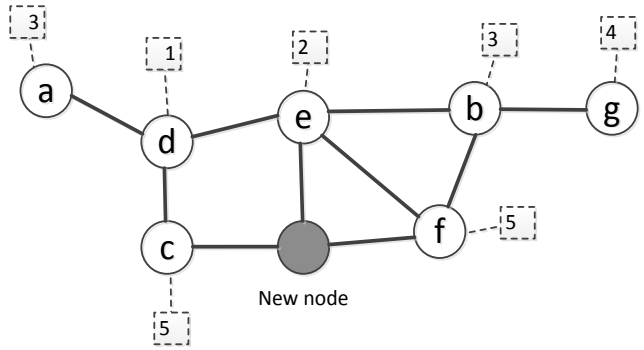

Fig. 8. Example of conflict an assigned time slot [1]

When a new node detects the conflict, it solves this conflict in the following procedure.

Dividing the assignment

If multiple slots are conflicting at the new node, these slots are divided to the nodes which have caused the conflict. In the example (fig. 9), conflicting slot 4 and 12 are divided to nodes *a* and *b* [1].

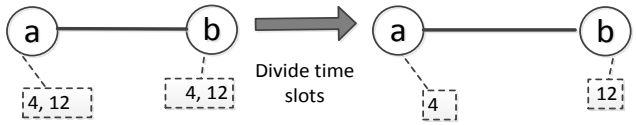

Fig. 9. Dividing the assignment of time slots [1]

Deleting a conflicting slot

If in the network are some un-conflicting slots assigned to nodes causing the conflict, the conflicting slot is released from all the nodes except for that with the smallest number of assigned slots (fig. 10) [1].

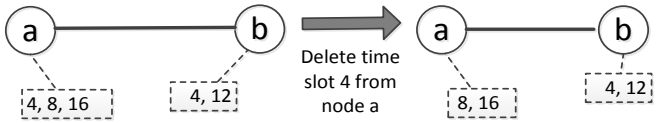

Fig. 10. Deleting the conflicting time slot [1]

Doubling the superframe and dividing the assignment

If the conflict occurs among nodes to which only one time slot is assigned, this conflict cannot be solved with the current superframe length. In this case, the superframe length of these nodes is doubled and the time slot assignment is divided in the doubled superframe. In example (fig. 11) the space for conflicting time slot is doubled by doubling superframe length. The space can be divided to nodes *a* and *b* [1].

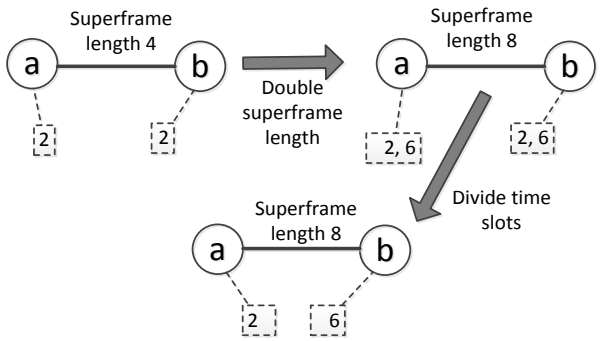

Fig. 11. Doubling the superframe and dividing the assignment [1]

After reconfiguring the time slot assignment, the new node sends SUG packet with the information on the reconfigured slot assignment and the selected slot. Neighboring nodes which have received this SUG packet also reconfigure their slot assignment and send REP packets with reconfigured information. The new node may fail to collect the information on the slot assignment correctly due to the collisions of INF packets. Then the new node sends the information on the slot in which collisions have occurred to all neighboring nodes instead of the SUG packet. Neighboring nodes of the new node, which have sent the INF packets in the conflicting time slot, retransmit the INF packets after waiting for certain superframes determined at random [1].

RELEASING TIME SLOT ASSIGNMENT

When a node exits from the network, it stops transmitting DATA packets and releases time slots assigned to itself. Neighboring nodes detect the exit of the node when no packets from exited node have been received during the time of the superframe length of the exited node. Then they release the time slot assigned to

the exited node from their time slot assignment information. They also release the time slots assigned to nodes that have gone out of their contention area due to exit of the node. After reconfiguring the time slot assignment, neighboring nodes of the exited node send the updated information to their neighboring nodes. The nodes which have received this information reconfigure the time slot assignment by releasing the time slots assigned to the exited node [1].

CONCLUSION

The paper presents the construction of the secure Ad Hoc sensor network protocol. The operation of this protocol is based on the ASAP protocol, whose efficiency measured in terms of the radio channel utilization is much larger than the USAP protocol [1]. The protocol described in this paper has been extended with additional functions related to data security (authentication of new nodes and encryption of data transmission), and the determination of the network hierarchy level of the reference nodes. Two new types of packets have been proposed: the authentication packet (AUTH) and the hierarchy level packet (LEVEL). The protocol is currently implemented on the hardware devices that will form the sensor network.

Acknoledgements

This work was supported in part by the Project DOBR-BIO4/058/13045/2013.

REFERENCES

[1] Kanzaki A., Uemukai T., Hara T., Nishio S., *Dynamic TDMA Slot Assignment in Ad Hoc Networks*, Proceedings of the 17th International Conference on Advanced Information Networking and Applications (AINA '03), Mar. 2003, pp. 330–335.

[2] Kanzaki A., Hara T., Nishio S., *An Adaptive TDMA Slot Assignment in Ad Hoc Sensor Networks*, Proceedings of the 2005 ACM Symposium on Applied computing (SAC '05), pp. 1160–1165.

[3] Stallings W., *Kryptografia i bezpieczeństwo sieci komputerowych. Matematyka szyfrów i techniki kryptologii*, translation A. Grażyński, Ed. Helion, Gliwice 2012 [*Cryptography and Network Security. Principles and Practice* — original title]].

[4] Young C. D., *USAP: a unifying dynamic distributed multichannel TDMA slot assignment protocol*, 'Proc. IEEE MILCOM', 1996, Vol. 1, pp. 235–239.

[5] Young C. D., *USAP multiple access: dynamic resource allocation for mobile multihop multichannel wireless networking*, 'Proc. IEEE MILCOM', 1999, Vol. 1, pp. 271–275.

BEZPIECZNY PROTOKÓŁ TRANSMISJI SENSOROWEJ SIECI AD HOC

STRESZCZENIE

W artykule zaprezentowano bezpieczny protokół radiowej sieci sensorowej Ad Hoc. Sieć ta pracuje w oparciu o metodę wielodostępu TDMA. Szybkość transmisji w kanale radiowym wynosi 57,6 kb/s. Przedstawiono budowę ramek, rodzaje pakietów oraz procedury uwierzytelniania, przypisania wolnych szczelin czasowych do węzła, zwalniania przypisanych szczelin i wykrywania konfliktów przyporządkowania szczelin.

Słowa kluczowe:
Ad Hoc, TDMA, ASAP.