Node to Node Watermarking in Wireless Sensor Networks for Authentication of Self Nodes

Hasan Farsi*
Department of Electrical and Computer Engineering, University of Birjand, Birjand, Iran
hfarsi@birjand.ac.ir
Seyed Morteza Nourian
Department of Electrical and Computer Engineering, University of Birjand, Birjand, Iran
nourian_morteza@yahoo.com

Received: 03/Aug/2013 Accepted: 12/Apr/2014

Abstract
In order to solve some security issues in Wireless Sensor Networks (WSNs), node to node authentication method based on digital watermarking technique for verification of relative nodes is proposed. In the proposed method, some algorithms with low computational for generation, embedding and detection of security ID are designed. The collected data packets by the nodes are marked using security ID. In the proposed method, header is used to mark the packets. Since the nature of the sensor networks is cooperative, using the head of the packets is proposed for authentication. Also using the marked head can prevent from sending and receiving fake data in the other nodes. Simulations have been performed in environments with imposing unrealistic data and having a probability from 1% to 10%. Comparing the proposed method with other methods shows that the proposed method in term of security, reducing traffic and increasing network lifetime is more effective.

Keywords: Watermarking, Wireless Sensor Network, Packets Head, Node, Information Security.

1. Introduction

Wireless Sensor Networks (WSNs) are developing networks that can play an important role in collecting and transmitting data. Application of these networks, especially in strategic areas such as border military districts that are not easily accessible, is highly in progress. Traffic control, healthcare, biotechnology and pharmaceuticals, rescue and military reports - security and espionage cases are some areas that WSNs are used [1,2]. WSNs are multi hop that have the shared nature and internal power management without any direct supervision [1,2]. These networks are constructed by many sensors that are called nodes in this article. These nodes are capable of sensing, gathering and transmission of information and communication together. Depending to some applications of these networks, the transmitted data between the nodes can be very sensitive and crucial. Due to the performance of these networks, there are many security challenges. This corresponds to emerging attacks resulted by bogus nodes and unrealistic information. (Some attacks are node capture and impose false routing information) [1]. Therefore, it is necessary to adapt appropriate procedures to ensure the information security is guaranteed.

In order to prevent the transmission of unrealistic information, a method is required to be applied to distinguish factual information. In fact, certification and authentication methods have to be used. In WSNs due to limitation of computation capabilities, energy, bandwidth and storage, conventional and traditional encryption methods using secret codes may not be implemented. Therefore, it is needed to use low complexity and more appropriate methods to verify the original information.

In this paper, a digital watermarking method for authentication of packets in WSNs has been proposed. Generally, watermarking is used to achieve two main objects; recognition of intangible property information and transmission of confidential information. In recent years, much research in the field of digital watermarking based on data such as audio, image, video and text and information resources, has been proposed in regular networks [3,5]. However, the limited research in this area has been conducted on WSNs [6,10].

In [6], an algorithm for generating the security ID for outgoing packets has been introduced. This identifier is embedded using the pre-defined embedded algorithm in the send-data packets. These packets are transmitted in the whole network and in central receiver station, the main packets are identified and their information is extracted. In [7], a watermarking technique is combined by imposing a series of restrictions during the operation of sensing and processing the information performed by the node. These limitations are appropriate with the encrypted identifier embedded in the data. In some methods, watermarking is only used to prevent unauthorized users to access the information [8], or to guarantee the completeness and detection of the received bits [9]. In some cases, the secure transmission of confidential information is discussed. This confidential data in accordance with the proposed algorithm in

* Corresponding Author

conventional data, before sending the message is embedded [10].

In all the presented methods, with some additional processing on each node, it is tried to increase data security but most of these methods have not considered the shared nature of network performance. In fact, only the sender node is considered and the presented methods are provided independently from other nodes. However, by considering the entire network, it is possible to propose more effective methods providing better performance.

In this paper, we propose a method to verify authentication and to indentify real packets sensed, received and transmitted by original nodes. In the proposed method, considering the nature and performance of WSNs, the packet header is used to embed the security ID. Using certain spaces of the packet header and a new embedded algorithm, the proposed watermarking is performed. At the receiver node, the packet header is examined and verified by the rest of the received packets. In some environments with having a possibility of forced fake packets, the proposed method increases network security, reduces energy consumption and network traffic, effectively.

In following section, the structure of used WSNs is briefly explained. In third section, the procedure of collection, packaging and delivering information in WSNs' nodes are explained. In section 4, the process of watermarking in the proposed method is explained. In section 5, the procedure of verification of packet authentication is demonstrated. Finally, in section 6, the obtaining results by applying the proposed method on WSNs are presented and compared with other methods.

2. Structure of Wireless Sensor Networks

WSNs consist of many sensors called nodes. These nodes randomly or based on a specific design are distributed in an environment [1,2]. These nodes are virtually classified based on their transmission range in each area.

In each cluster, according to the amount of energy belonging to the node, the center of the cluster is selected and other nodes either directly or via other nodes of the cluster are connected to the center of the cluster.

These clusters and the centers are not fixed and during the different business cycle of the network may vary. Network information is transmitted to the main station and sink through the centers of the clusters. In Figure 1, a simple exponential segmentation of different clusters is shown. These clusters are connected to each other through the centers or the boundary nodes [1,2].

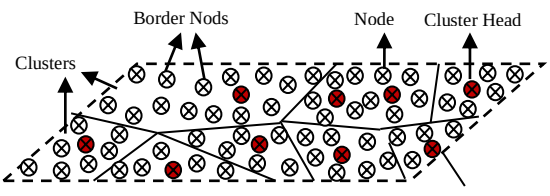

Fig. 1. WSNs' nodes divided into different clusters

3. Collecting, Packaging and Sending the Data

The standard "Zigbee / IEEE 802.15.4" is normally used in WSNs. With respect to this standard and the models presented in [6,10], we propose a new model for packaging the information in the network nodes. A new pattern packet by nodes is given by:

Packet = (Head, Send-Data)

Each packet is divided into two parts; the first part is packet header or Head and the second part is called transmission information or Send-data. The packet header contains some information such as the routing information, packet length and other parameters in the standard "Zigbee/IEEE, 802.15.4". The send-data contains the pre-defined information which is needed to be transmitted by the nodes in each time period. It is assumed that each node collects the information in the "kth" cycle. This information is collected and stored in two forms by the node; first, the sensed information by the self-node from its surrounding environment and second, the received packets from other nodes and their authenticity has been verified. If the information is sensed by self-node, each packet is in form of Si= (t, d1, d2, ...,dn). In this packet, "i" refers to the cycle of working nodes in the sense of [(i=1,2, ..., m), m≤ k. "T" refers to the time of sensing information. [Dj, (j=1,2, ..., n)] indicates the parameters that must be sensed by the node. The general pattern of the packets is in form of (N, S1, S2, ..., Sk, D), where "N" indicates identification of the node in the network or ID, and the "D" specifies the length of each packet. If the packets are received from other nodes and their authenticity is verified, they have different parameter of N. In fact, these packets are packaged in the other nodes with the same pattern, except that N contains the node ID which has sensed its surrounding information, primarily.

The packet transmission time by the nodes has to be defined for all nodes. For example, in [6,10], it is assumed that the transmission is performed when the storage is fully loaded. However, due to defining a new model for the packets, the packet transmission time can be performed in specific time intervals. By sending packets scheduled times, network can plan better programming. In addition, some nodes in the network can sense and transmit information both. Therefore, the criteria of fully loading storage can decrease network performance. The reason is that the nodes located in optimum direction of information transmission are unable to receive new packets from other nodes while their storages are not fully loaded even they have performed their duties in time intervals. This problem is due to being the same nodes in WSNs, and therefore the storage capacity is the same for all nodes. If transmitter node sends the information when its storage is fully loaded, then the storage of receiver node should be unloaded to be able to receive the information completely; otherwise the information has to wait until the receiver node located in optimum direction of information transmission sends its

data and then by unloading the storage it could receive the information. This problem, due to being several nodes in the network, may destroy or create unreasonable delay in the sending the packets and the network performance will be degraded. Meanwhile, it increases the traffic in optimum direction of transmission. However, if the transmission time is scheduled, then the nodes are able to sense and store the surrounding information and also to receive the packets transmitted by other nodes at the same time.

At a period of time until reaching to retransmission time by the nodes, if the packets are completely received by the node they are packaged and sent on time. But if the packets are not completely received, they are stored in a part of storage and after complete receive, they are packaged and transmitted in the next period time. The transmission time periods are selected such that the transmission is performed before the storage is fully loaded. Moreover, the time period should be set so that the nodes have appropriate transmission rate based on the length of the header and the amount of transmission data packet. For example, the time period should not be considered too low such that the amount of transmission data packet compared to the length of the packet header is unusual. Thus, the transmission time periods are determined based on the type of nodes, the network workspace, request information from the network nodes and the storage capacity. With regards to appropriate timing, it is possible reduce network traffic and delay. By achieving the coordination between the transmission and receive time of packets at the nodes, the appropriate timing is obtained.

If the measure of information transmission time at the nodes is full-load storage, sometimes the traffic increases around the nodes located in optimal routes and especially in the cluster centers. However, it is possible to control the traffic by proper timing. In Table 1, two measures of information transmission time are compared. For this comparison, a working period, "T", is considered for information transmission for each node, and a fixed amount of data is sent by the network. These nodes send data at the same rate for the first stage by the measure of full-load storage and in the second stage with defined schedule. This comparison has been performed based on this reality that in different time periods in the grid, the number of packets that have been transmitted but not yet received, both criteria are calculated. It has been assumed that there are 35 nodes and one cluster center. In first step, the length of each bit stream, 100Kbit has been assumed and in the second step, for each 0.1T, the nodes transmit the data in 8 stages. During the 8 stages, the size of the transmitted data is as same as the first step. The transmission rate is 50kb/s for each node and bit transmission is based on Poisson distribution. For convenience in computing, the total information sent to the network is limited and the traffic in both steps has been considered to be fixed. In the first step, the time of full-load storage is considered to have an exponential distribution and totally production and distribution of the packets on the network trend to Gaussian distribution. Therefore, the nodes located in transmission path receive higher information and include higher traffic. Thus, these nodes have to send the information in shorter time intervals compared to the other nodes and they are time scheduled according to the network conditions. This comparison is intended to provide a time 5 minutes and the number of packets is counted in every 30 seconds.

Table 1. Number of packets not received on the first and second tests

Number of packets in the second stage	Number of packets in the first stage	Calculation time of un-received packets
0.1 T	4	10
0.2 T	22	16
0.3T	29	14
0.4 T	38	15
0.5 T	36	12
0.6 T	39	15
0.7 T	22	13
0.8 T	10	14
0.9 T	3	12
T	-------	-------

According to the table, by the assumption that none of the packets has not been lost by traffic and the delay, it is observed that the transmission and receive of information has better coordination in case of scheduled times information. It should be noted that the number of packets has the same length in the first stage but in the second stage they have variable lengths and in some cases much smaller than the first step. For example, at "0.1T", the number of bits of 10 undelivered packets is 350kbit which is approximately equal to 3.5 packets in first step.

As observed, the first stage has more changes compared to the second stage. These changes sometimes correspond to create traffic and sensible delay in the network, and in some cases can cause data is lost. The traffic in wireless sensor networks is one of the main factors for identification of key nodes, especially center of the clusters. By identification of the location of such nodes, communicating and accessing information is easily performed. It also increases the chance of attacks to the network which even incapacitates the entire network [1,2]. By scheduled times, packaging and proper timing between the sending and receiving packets, the packet congestion around the center of the cluster and probability of location identification decrease. In section 6, the impact of this type of packet scheduling operations in watermarking is fully investigated.

According to the new paradigm of packaging and sending data, the packets sent by each node contain multiple nodes. After receiving the packets, the base station extracts and saves the information of each node according to characteristics of "N" and "D" intended for the node in the network and the business cycle.

4. Process of Watermarking at Receiver

In this section, before indicating the proposed method, in order to generate and embed the security ID of data

packets, a brief discussion on use of packet header as the location of embedding security ID is presented.

4.1 Using packet headers for watermarking

In this article, regards to the packet header differs in different nodes and the packets lose their headers by passing through different and they are replaced by new packets with new packet header, the packet headers are used for authentication of packets.

The main reason for using the packet headers is that due to nature of WSNs it is not required the authentication to be only performed in the base station. In most proposed method so far, the transmitter node has been only considered and the nature of communal belonging to the WSNs has not been used. Since each node placed in transmission of the packets can perform the authentication. Because the data is sent through a node, if the client node is able to detect the original information from the fake information then it can remove fake information, receive the original data and save it in transmission information part of the new packets. Using this trick result in reduction of traffic and congestion of the packets around the nodes, especially center of clusters located in optimum pathways and prevents occurrence of the attacks resulted from the network traffic, such as, traffic analysis. Moreover, the consumed energy for receiving one bit in each node is about 0.5µj and for transmission is about 1 µj [1, 6, 10]. Therefore, if the authentication of the information is checked in base station and the information is fake, in this case, all the nodes placed in communication path to base station have to consume a lot of energy for receiving and transmission of the information which is actually fake. This is unacceptable due to energy constraints in the nodes. On the other hand, the transmission information part of the packet may contain several hundred bytes and if the security ID is supposed to be embedded in the transmission information part and it is assumed that the authentication is checked node-to-node, all the nodes have to receive many bytes for authentication of real or fake information. In this case, the consumption of the energy by the nodes increases. For better performance of the network, it is required to propose a strategy in which the client nodes can decide to send or block the information by consumption of minimum energy. Although using packet header for watermarking in other networks except WSNs seems inappropriate due to its change in different transmission stages, in WSNs the transmission of the packet is in cooperation with the other nodes and the overall patterns are similar, using the packet headers for watermarking can be appropriate. Thus, it is possible to use the packet header as a proper choice to verify the ownership. In each node, firstly, the header part of the packet which has a length much smaller than the transmission information part is received and then the authentication operation is performed. If it is right and original, the rest of the packet is received, otherwise the packet is fake and it is discarded.

4.2 Watermarking process

As mentioned in the previous section, incoming packets with sensed data are stored in the data packet transmission part, and a new header with the new security ID is sent. Figure (2) shows the watermarking process in the sender node. According to Figure 2, the sensed information in different working cycles of the node with the received packets from other nodes is packaged. Packaging in each period is stopped when there is enough time for executing watermarking algorithms until arriving the transmission time. According to standard "Zigbee/IEEE802.15.4", packet header in stop time of packaging with network information is formed. By forming the packet header, the algorithms (1) and (2) (which are defined in section 4.2.1) are performed. The result of the algorithm (2) is a new header which contains the security identifier, and proves the authenticity of packet ownership in the client nodes. Embedding the security ID is performed such that in watermarked header, the original header information is maintained. It is obvious that since the security ID of the packets change in every stage the network security considerably increases.

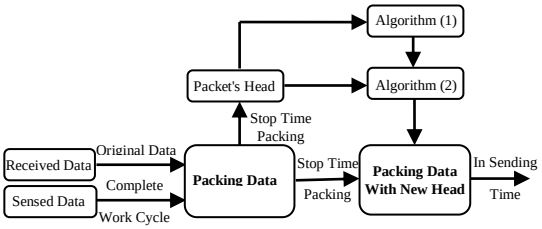

Fig. 2. The watermarking process for sender node.

By new definition of information packaging in the nodes and similarity of the nodes in WSNs, some defined fields in the header seem to be insignificant. For example, the field of the sender node, according to the standard “zigbee”, has allocated 2 bytes for header. As noted, the transmission information part contains the sender's node ID. Meanwhile, according to the standard, some header fields can provide some void bits. In this study, we try to embed the security ID using these fields. This is achieved such that the information in the header is maintained. In fact, in this methodology, the header information is not manipulated and only security ID bits are embedded in the void and least significant bits of the header which are defined in both the transmitter and receiver nodes.

Now, we are encountered with two issues; first, how to produce secure ID, and second, how to embed the Security ID.

4.2.1 Generation of security ID

First, the packet headers are divided into two parts according to the standard used. The first part consists of some fields which remain unchanged and its information has been used generate the security identifier. In this article, these fields are called fixed fields of header. The second part consists of some fields such as the field related to the sender node or tab ratings, which are either

less important or can include more number of bits compared to the fixed fields of header. In these fields it is possible to define a number of void bits, which their places are known in the receiver and the transmitter. These fields are called variable fields. This part is used to embed the security ID bits.

In order to generate the security ID bits, the proposed algorithm in [6], has been used but with a slight change in the algorithm, a "Hash" function is applied. The "Hash" functions generate a unique output by receiving the specific inputs under predefined conditions. One of the inputs to the hash function is the number of bits, "L", which is considered as a security ID and it is shared in all nodes. Other input is a security key, "k", which is a prime number and it is shared automatically in all nodes. The certain bits of the fixed fields of header which are known in both sender and receiver are the other input. This input causes that the probability of generation of fake security ID considerably reduces due to being difference of headers in different stages of transmission. Note that this algorithm is executed only when the header is received. Because the fixed fields and other parameters are transmitted without any changes in all nodes. The hash function generates a bit string as a security ID only by simple operations. The security ID generation algorithm has not to be simply detectable, to be low complexity.

Algorithm 1. Generation of security ID bits

/ / Initial data k, L
1) fix = constant values in header fields
2) w = LSB (fix)
3) WM = Hash [L, k, w]

4.2.2 Embedding the security ID

The output of Hash function, WM, is a L-bit string. This bit string has to be placed in variable fields of header. First, the bits in the variable header fields that are marked to embed the bits of security identifier are numbered sequentially. This numbered bit string is indicated by "d", where d(i) refers to ith bit of the bit string. The length of WM-bit string can reach to tens of bits. However, as will be shown in Table 2, an 8-bit string can also meet the security expectations.

Algorithm 2 shows the process of embedding the security ID bits. The algorithm includes the property of rotational placement and security ID may not be easily detected and recovered. An important feature of this algorithm is non-interference in the placement of information in the header.

After construction of the new bit string, d, the sign bits are placed in the variable fields of header according to the specified numbers, and the information with the new header is then transmitted.

Algorithm 2. Embedding WM bits in "d"

/ / Initial data k, L
1) len = length (d)
2) For j = 1: L
p = [j * k / len]
mod = j * k mod len
if p + mod <len
d (p + mod +1) = WM (j)
else
d (p + mod-len +1) = WM (j)
End if
End

5. Verification and Authentication of Packet Ownership

After transmission of the packets by the sender node, it is firstly needed to verify the authentication of packet ownership in client node and then to be fully downloaded. Figure 3 shows the receive process in client node. In client node, the header of the packet is fully received and then the algorithm 1 is executed. Since the fixed fields of header remain unchanged, the algorithm 1 in the receiver and the transmitter has similar results. After receiving the header, the sign bits in the variable fields of header are extracted.

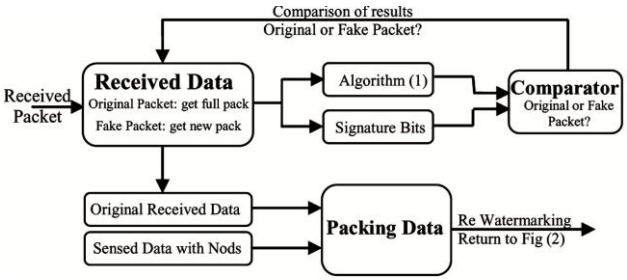

Fig. 3. Block diagram related to verification of authentication of packet ownership in client node.

According to the algorithm 1, WM-bit string is generated based on fixed fields of header. Then, based on pre-defined location of the sign bits in the receiver and the transmitter, the bit string, d, is extracted. Next, the bit string of WM' is extracted from bit string of d' by reverse operations. By comparing WM and WM ', the received packet is verified whether original or fake. This procedure is performed based on algorithm 3. If the packet is original, the remaining information of packet is received otherwise the packet is removed from the receive cycle and discarded. In order to compare WM and WM ', we use a measure which indicates virtual difference between WM and WM ' [6]. This measure is practically obtained by consideration of environment and probability of error created by the environment. After verification of being original or fake packet, a command is sent to the receiver node. If the packet is original, it is commanded to the receiver node to continue receiving the packet. However, in case of detection of fake packet the remaining information of packet is not received and it is commanded to the client node to receive another packet header. After receiving the original data, if the packet transmission information is fully received, the information is sent to the packaging part of the node. Meanwhile, the node information sensed in different business cycles is transferred to packaging part of the information. From this stage onwards, if the information is needed to be embedded, the watermarking is re-performed as shown in Fig. 2.

Algorithm 3: Security ID bits extracted

```
/ / Initial data k, L and t values of allowable error
1) The Algorithm (1) WM Production
2) Len '= length (d');
3) For j = 1: L
        p = [j * k / len ']
        mod = j * k mod len '
              if p + mod <len '
                  WM '(j) = d' (p + mod +1);
              Else
                  WM '(j) = d' (p + mod-len +1);
          End if
End

4) E = sum (Xor (WM, WM '))
5) If E <t
        Accept data
    Else if E> t
        Reject data
    End if
```

6. Applying the Proposed Method on Wireless Sensor Networks

As noted earlier, the proposed method provides acceptable results in the environments containing fake packets. In this section, the existing security in the proposed method is discussed. Then, network traffic analysis and energy consumption will be discussed. In the analysis, it is assumed that all the nodes are imposed by 0.01 to 0.1 fake packets. The process and transmission rate of the packets are similar to the assumptions in section 3.

6.1 Security of the proposed method

In this method, a harmonic function is used such that its process is not simply recognizable. Since the input of the function is the security key which is inaccessible, the probability of fake WM generation is quite low. In addition, the state of placement regards to varying WM in different nodes causes to increase the security of the received packets. If an undesired system is going to produce fake header and ID which is undistinguishable by the network, it is required to consider huge aspects. It should be noted that since the header information of each packet belonging to the packet itself, is used for generation of ID, the ID of the packets differs even they are generated in one node. Since undesired system is unaware about the parameters of "l" and "k" and the process of ID generation in the nodes, it can assume that the probability of correct generation of ID for each bit is 0.5. Since the information of the fixed header fields is used for generation and authentication of ID at receiver, due to being difference between the headers in various stages of sending headers, the probability of generation of fake ID highly reduces. If the total length of the header is n-bit, the probability of generation of fake ID compatible with the original ID is multiplication of the probability of finding the L-bit location of ID in header and the probability of correct ID. This is given by:

$$p(n,L) = \frac{1}{\binom{n}{L}} 0.5^{L} = \frac{L!(n-L)!}{n!} 0.5^{L} \quad (1)$$

Table 2 shows the probability of fake ID for different values of n.

Table 2. The probability of fake ID with length of 8 bits

n	L	P(n,L)
48	8	1.04×10-11
56	8	2.75×10-12
64	8	8.83×10-13
72	8	3.27×10-13
80	8	1.35×10-13
88	8	6.08×10-14
96	8	2.95×10-14
104	8	1.52×10-14
112	8	8.22×10-15
120	8	4.65×10-15
160	8	4.38×10-16
200	8	≅ 0

It is observed that by choosing only 8 bits for the ID and watermarking the probability of generation of fake ID considerably reduces. It seems that due to variation of the ID during the transmission process, 8 bits provides the network security expectations. However, using less bits results in lower complexity and lower costs for transmission.

The most important factor in authentication methods is the accuracy of correct verification of original packets such that neither the original packet is discarded nor the fake packet is received. Figure 4 represents the percentage of detection for the original and fake packets. The upper curve represents the percentage of received original packets to the total original packets and the lower curve illustrates the percentage of received fake packets to the total fake packets. In this experiment, n=72 and the results for different values of L are examined.

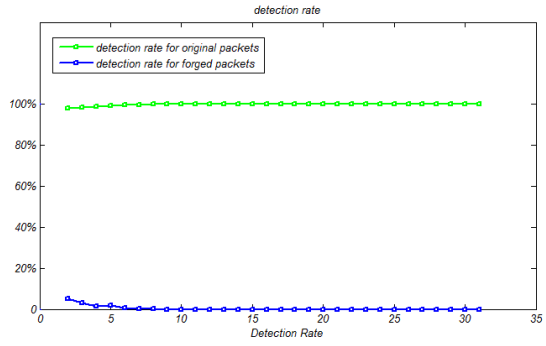

Fig. 4. Percentage of received packets for original and fake cases.

It is observed that if the number of bits for WM is more than 8 bits, ideal results are achieved. Compared to [6], although the methods are very different but they have the same results for more than 4 bits.

Therefore, according to Tab. 2 and Fig. 4, the proposed method can provide the required network security expectations. Meanwhile, the security identifier produced and embedded by the proposed method contains lower number of bits compared to other methods [6].

6.2 Network traffic analysis

One of the main methods used by the foreign system to detect the location of the nodes is network traffic analysis. By the network traffic analysis the location of the nodes placed in strategic areas or the position of cluster centers in the optimal transmission paths are identified. This provides different attacks such as wormholes, sinkhole attacks and node compromising to be imposed to the network [1,2]. The two-step proposed method can reduce network traffic. The first step consists of the new definition of packaging and scheduling packets and second step includes using the headers for watermarking and authentication of the packets. It is obvious that traffic reduction causes reduction of delay in transmission of the information in the network.

Fig. 5 shows the proposed method against the method in [6,10] for packaging and information transmission in terms of the number of packets existing in queue in different time intervals. These results have been obtained by computation of the number of packets produced in the node for each time interval independent of previous time interval. In this procedure, some nodes obtain the necessary bandwidth to send the packets in the time interval generated and some other nodes, due to limitation of bandwidth, are unable to send the information. In this case, the generated packets which have not been transmitted, stay in transmission queue and the node, as soon as accessing to the necessary bandwidth send them. The number of packets stayed in the queue for each time interval is:

$$P_P - P_T = P_Q \quad (2)$$

Where the PP indicates the number of packets generated in each time interval, PT, is the number of generated packets which have been transmitted at the same time interval and PQ is the number of generated packets which have been stayed in queue. PQ is calculated at each time interval. The percentage of ratio of PQ to PP has been shown in Fig. 5. These values represent the percentage of packets which stay in queue at every time transmission. Obviously, higher values represent higher network traffic and delay. These results have been only obtained for the impact of packaging and information transmission patterns in network traffic and the watermarking applied in the proposed method and in [6] has not been considered in the simulation.

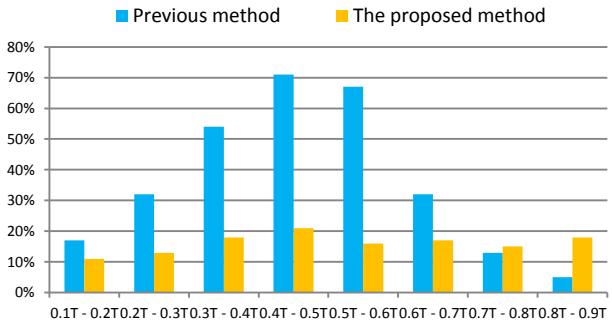

Fig. 5. The amount of queued packets per time slot

According to Fig. 5, if a criterion is filling storage [6.10], the ratio of PQ to PP increases in some time intervals. The reason is the packet congestion in some intervals and the limited bandwidth. The limitation of bandwidth has to be considered as one of the fundamental challenges in this type of network where the transmission delay is important. Inattention to bandwidth limitation causes packet loss and node information. The congestion of nodes which do own transmission as soon as filling the storage increases and consequently the number of packets prepared for transmission increases. In this case, some packets are sent at generated time and some packets stay in queue to be sent at next time intervals with having the required bandwidth. Regards to assumption of Gaussian distribution, the congestion of generation and transmission of the packets increases in median time intervals and non-transmitted packets affect the transmission in the next time intervals. Therefore, for median time intervals between (0.3T-0.6T), the number of queued packets greatly increases. Since the traffic load and the amount of information for transmission have been considered the same for the proposed method and the method presented in [6,10], as observed in Fig. 5, the method in [6,10] packs and transmits the desired information and therefore the generation and the congestion of the packets reduces in the final time intervals and the nodes have higher bandwidth for transmission of remaining packet in the network. The important issue is that the network traffic has to be controlled such that key nodes cannot be identified and with the fluctuations in the density of traffic and the congestion of packets for transmission, the network may be disordered.

According to the new model packaging as shown in Fig. 5, it is observed that with having the timing for transmission and appropriate pattern for packaging, the number of queued packets for transmission, even in high congestion time, is almost unchanged. In other words, with accurate timing for information transmission, it is possible to reduce the delay and prevent fluctuation of network traffic at different time intervals.

Figure 6 compares the proposed method with the method presented in [6]. The comparison is based on the freed bandwidth in each area of the network, without applying the watermarking. The number of nodes is variable in each area and the results have been obtained

regards to different number of nodes. For each number of nodes, the first column and the third column are related to the method presented in [6] and the proposed method, respectively. In the second column, the watermarking method presented in [6] in combination with the new model of packaging and information transmission has been shown. In fact, the second column indicates the effect of the new model applied on [6] in reduction of network traffic. For example, if there are 50 nodes in center of a cluster, the proposed method regards to imposing the percentage of the fake packets, is able to free 14% of occupied bandwidth compared to without applying watermarking case. This reduction is more sensitive in strategic areas. For two reasons, the proposed method provides better performance; first the procedure of packaging and transmission and second prevention of fake packets distribution in the network. For example if the fake packets are received and distributed in an area with 50 nods (sending the packets in the network broadcast is assumed as broadcast), they are received and sent many times until reach to cluster center several times and they are finally discarded in base station. However, the proposed method is able to verify and discard the fake packets in primary step from the send-receive cycle and therefore increases the bandwidth for transmission of the original packets.

The calculation is based on computation of the amount of information which has been sent and received in the network regards to the amount of fake information for different time intervals. The ratio of the obtaining values to the case without watermarking are calculated and shown in Fig. 6. The different values in different methods can indicate as free bandwidth by applying the related methods.

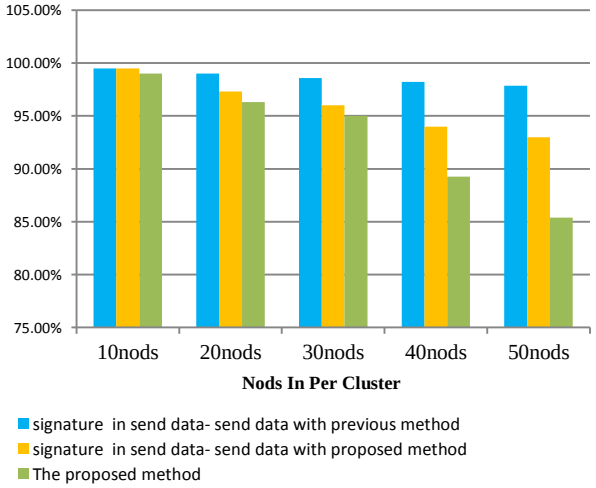

Fig. 6. Occupied bandwidth in different methods with and without watermarking

6.3 Evaluation of energy consumption

One of the important issues that have a large impact on the performance of each method in WSNs is the problem of energy consumption. As referred before, the proposed method is appropriate when the probability of imposing fake packets exists. As the probability increases, the proposed method provides better performance, especially in terms of energy consumption and traffic reduction. Since the energy consumption of the nodes for sending and receiving the bits is more than internal process applied on the bits, although extra processing is performed by the proposed method in each node, by discarding fake packets from send-receive cycle not only the consumed energy resulted by extra processing is compensated but also some energy is stored in the node. This increases the longevity of the network and provides better performance. Reduction of the traffic caused by the proposed method also has a direct effect on reducing energy consumption by the nodes. Figure 7 indicates the amount of consumed energy by the proposed method in comparison with the method presented in [6]. This has been achieved based on computational models discussed in [6.10]. The only difference is that this has not been achieved for only one node and has been obtained by averaged total impact of traffic in each area. For authentication of packets in [6], energy consumption of each node slightly increases compared to the case without watermarking but in the proposed method, due to accurate transmission timing and the number of nodes in each area, the energy consumption of each node even decreases. In Figure 7, for different scheduling in the network, the amount of consumed energy for variable number of nodes in each zone has been calculated. The effect of traffic reduction on reducing energy consumption is quite clear. The experiment assumptions are similar to the previous example. There are several points which are briefly mentioned:

First, for low number of nodes in each area, the consumption of energy is slightly higher by the proposed method. The reason is reduction of packet numbers and low transmission rate. Due to being smaller length of packets compared to other methods, it is required to send a packet header for each packet which causes low rate transmission of information and for similar amount of information; it is needed to consume more energy. However, as observed in Fig. 7, this problem is slightly removed by increasing the transmission time.

The second point is the effect of traffic on reducing the consumption of energy. As observed, by increasing the number of nodes in each zone, the averaged energy consumption of the nodes reduces compared to the case of without watermarking. According to the description given in section 6.2, the proposed method can reduce the network traffic compared to the case without using watermarking. Obviously, by increasing the numbers of nodes in the network, the number of send and receive packets increases. If the fake packets are distributed in the environment containing wireless sensor network and there is not a criterion for verification of the fake packets, due to increasing the number of nodes and the information consequently, the number of fake packets and undesired information increases in case of unused watermarking and

therefore more energy is consumed by the network. As shown in Fig. 7, by increasing the number of the nodes, the proposed method is able to decrease the consumed energy approximately 15% compared to the case without using watermarking.

The third point is that by increasing the transmission time such that the performance of the network is not been affected, the energy consumption more reduces. The major reason is increasing the packet length with increasing duration of time. As a result, the information transmission rate is higher and the amount of desired information is transmitted by lower number of packets. It has to be mentioned that increasing the time duration more than a certain threshold results in more delay and more congestion of the packets in the network. Therefore, it has to select the most appropriate procedure for transmission of information by a balance between all conditions and restrictions.

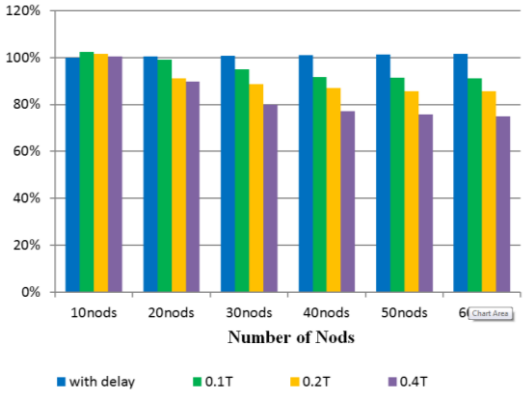

Fig. 7. Analysis of energy consumption in each area

7. Conclusions

In this paper, due to the shared nature of sensor networks, we proposed a method which provides acceptable results in terms of safety, traffic and energy consumption.

The proposed technique in the environments with a high risk of attacks provides better results than existing methods. In environments with very low probability of attacks and secure environment, the proposed method imposes additional processes leading to reduction of network performance. However, for the non-secure environments, the proposed method through relatively light processing and therefore low complexity provides considerable security for the network. Furthermore, in spite of general methods, the proposed method results in positive effects on the network lifetime. The new model for packaging and transmission of information applied in the proposed method provides the network the capability of time programming for sending and receiving the information. This reduces delay in data transmission.

References

[1] Misra, S.; Woungang, I.; Misra, Ch.S. “Guide to Wireless Sensor Networks.”;Springer-Verlag London Limited 2009.

[2] Tse, D.; Viswanath, P. “Fundamentals of Wireless Communication.”; Cambridge University Press 2005.

[3] Yin, H. C.; Lin, F. Q.; Ding, R. “A Survey of Digital Watermarking.”; Journal of Computer Research and Development, vol.42, no. 7, pp. 1093-1099, 2005.

[4] Agrawal, R.; Kiernan, J. “Watermarking relational databases.”; in Proceeding of the 28th VLDB Conference, Hong Kong, China: VLDB Press, 2002, pp. 155–166.

[5] Sion, R.; Atallah, M.; Prabhakar, S. “Rights protection for relational data.”; in Proceedings of ACM SIGMOD, San Diego, CA, USA: ACM Press, 2003, pp. 98–109.

[6] Dong, X.; Li, X. “An Authentication Method for Self Nodes Based on Watermarking in Wireless Sensor Networks.”; Networking and Mobile Computing, 2009. WiCom '09. 5th International Conference 24-26 Sept. 2009; pp: 1- 4.

[7] Feng, J.; Potkonjak, M. “Real-time watermarking techniques for sensor networks.”; in SPIE Security and Watermarking of Multimedia Contents, Santa Clara, CA, USA: SPIE Press, 2003, pp. 391–402.

[8] Sion, R.; Atallah, M.; Prabhakar, S. “Resilient rights protection for sensor streams.”; in Proceeding of the 30th VLDB Conference, Toronto: VLDB Press, 2004, pp. 732–743.

[9] Guo, H.; Li,Y.; Jajodia, S. “Chaining watermarks for detecting malicious modifications to streaming data.” Information Sciences, no. 177, pp. 281–298, 2007.

[10] Xiao, X.; Sun, X.; Yang, L.; Chen, M. “Secure data transmission of wireless sensor network based on information hiding.”; in Proceedings of The Fourth Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services. Philadelphia, PA, USA: IEEE Press, 2007 ,pp. 1–6.

Hasan Farsi received B.Sc and M.sc degrees from Sharif University of technology, in Communication engineering in 1993 and 1995, respectively. Since 1995, he was employed in university of Birjand as an academic staff. He was entered as a Ph.D student in Center for Communications Systems research (CCSR), University of Surrey, UK, in 1999 and received the Ph.D degree in communication Eng. in 2003. Since 2003, he was re-employed in university of Birjand and at the moment he works as associate professor in department of electrical and computer eng., university of Birjand. So far he has published more than 20 journal papers, 25 conference papers and a book titled “Time variable PDF presented by neural network” in 2013. Also, he is a member of scientific committee in three international journals and reviewer of IET. The interest areas are signal processing, speech processing, image and video coding.

Seyed Morteza Nourian received B.Sc and M.Sc degrees from Islamic Azad university of Najaf abad and University of Birjand, in 2010 and 2012, respectively. At the present time, he works as an invited lecturer in university of Najaf abad, Isfahan in department of electrical and computer engineering. So far he has published one journal and two conference papers. The interest areas are speech processing and wireless sensor networks.