Security Model for Tree-based Routing in Wireless Sensor Networks: Structure and Evaluation

Iman Almomani[1] and Maha Saadeh[1]
[1] Computer Science Department, King Abdullah II School for Information Technology,
P.O. Box 13835, The University of Jordan, Amman 11942, Jordan
[e-mail: i.momani@ju.edu.jo, saadeh_m87@yahoo.com]
*Corresponding author: Iman Almomani

Received January 21, 2012; revised March 13, 2012; accepted March 27, 2012; published April 25, 2012

Abstract

The need for securing Wireless Sensor Networks (WSNs) is essential especially in mission critical fields such as military and medical applications. Security techniques that are used to secure any network depend on the security requirements that should be achieved to protect the network from different types of attacks. Furthermore, the characteristics of wireless networks should be taken into consideration when applying security techniques to these networks. In this paper, energy efficient Security Model for Tree-based Routing protocols (SMTR) is proposed. In SMTR, different attacks that could face any tree-based routing protocol in WSNs are studied to design a security reference model that achieves authentication and data integrity using either Message Authentication Code (MAC) or Digital Signature (DS) techniques. The SMTR communication and processing costs are mathematically analyzed. Moreover, SMTR evaluation is performed by firstly, evaluating several MAC and DS techniques by applying them to tree-based routing protocol and assess their efficiency in terms of their power requirements. Secondly, the results of this assessment are utilized to evaluate SMTR phases in terms of energy saving, packet delivery success ratio and network life time.

Keywords: Authentication/Integrity, energy-efficient; network security, tree-based routing, WSN.

The authors would like to thank the anonymous reviewers for their valuable comments which improved the quality of this paper and clarified many important points to the reader.

http://dx.doi.org/10.3837/tiis.2012.04.016

1. Introduction

Due to the significant use of WSN in many sensitive fields such as health care and military applications, maintaining data security becomes a major challenge in the implementation of WSNs protocols. In such applications, it is important to consider security issues and possible threats in any protocol design. Breaking data security not only diminishes its importance, but it also affects the application objectives by providing false alarms and wrong reactions. Moreover, any security solution should consider the resource limitations of sensor nodes in terms of energy, memory and processing capabilities.

In this paper, energy efficient Security Model for Tree-based Routing protocols (SMTR) is proposed. The main contribution in this paper is the design of a security model that can fit in any tree-based routing protocol. This model consists of two modules; the first module is used in the topology construction process and it aims to ensure that the constructed topology is secure and safe to be used for data transmission. The second module is used in the data transmission phase to secure the transmitted data packets. To reduce the consumed energy in the data transmission phase, a fuzzy inference system is used to decide how to secure the transmitted data packets in the second module. The decision of the fuzzy system is based on three factors; sensor energy, time from last association process, and data status. The use of each factor will be discussed in details through the paper.

In addition to the proposed security model, we evaluate different security techniques to assess their power efficiency. This evaluation allows system designers to choose the best security technique that fits their systems' requirements. The studied techniques are grouped into three categories; MAC techniques which are CBC-MAC, XMAC, CMAC, and HMAC, digital signature techniques which are RSA and ECDSA, and block cipher techniques which are AES, RC5, Skipjack, and XXTEA.

The rest of this paper is organized as follows: related work is summarized in section 2. Section 3 presents an overview of tree-based routing protocols. Section 4 discusses the proposed security model (SMTR) in details. Cost analysis of SMTR model is discussed in section 5. Section 6 discusses SMTR evaluation and simulation results. Finally section 7 concludes the paper and presents possible directions for future work.

2. Related Work

Many secure routing protocols have been proposed for WSNs, nevertheless, limited researches have been carried out to solve the problem of securing protocols based on tree architecture. In this paper, a security framework is proposed to secure tree-based routing protocols by securing both tree formation and data transmission phases. The reason behind choosing tree-based architecture for our framework is its efficiency in terms of reducing excessive messages and the overhead in path searching and table updating, which makes this architecture suitable for lightweight networks. In this section a summary of tree-based secure protocols is presented including some researches that focus on the evaluation of different security techniques.

In [1] armor leach protocol is proposed to secure the LEACH protocol by proposing authentication, confidentiality and integrity security mechanisms. Another security framework is proposed by [2], they described two different scenarios for infrastructure and infrastructure less WSNs environment.

In [3][4] the authors use biometric-based authentication scheme. In this scheme two or more sensors measure the same biometric and find a specific value. This value can be used as a shared key or sent to the sink node to perform the authentication process. One disadvantage of biometric-based authentication is that sensors must be synchronized in order to measure the value at the same time. Another disadvantage is that all sensors should measure the same biometric which is not always true. In [5] three security services are defined. These services are authentication, confidentiality, and replay attack protection. The authors utilize three bits in the TinyOS packet format to support the three services. Each bit is assigned to one service. When a service needs to be applied, the packet format should be modified to support the applied service. The disadvantage is that this technique is platform dependent and can only apply on sensors with TinyOs platform.

In [6] the author studies the impact of adding message authentication code on the life time of wireless sensor network based on different symmetric and asymmetric approaches. The results show that the lifetime of a sensor node is almost not affected by the addition of authentication. In addition, the results show that using symmetric based authentication is more efficient than asymmetric approaches. However, this work does not consider energy factor in its comparisons.

In [7] the authors proposed a secure routing for tree based networks by ensuring authentication and confidentiality using one way hash chain and preloaded key. A sink-rooted tree is constructed to be used in the routing process. To ensure authenticity of the transmitted data, all the intermediate nodes must be initialized with the basic one-way hash chain number during the tree construction. The authors assume that none of the nodes could be compromised during the tree construction. Another protocol to secure tree-based routing is proposed in [8]. This protocol uses Public Key Cryptography (PKC) to protect the network against sinkhole attacks by signing the message to prove the identity of its creator.

For security techniques evaluation the author in [9] studied the impact of adding message authentication code on the life time of wireless sensor network based on different symmetric and asymmetric approaches. The results show that the lifetime of a sensor node is almost not affected by implementing the authentication. Furthermore, the results show that using symmetric based authentication is more efficient than asymmetric approaches. However, this work focuses only on IEEE 802.15.4 AES-CBC-MAC symmetric approaches in its evaluation. In [10] and [11] the authors presented asymmetric based authentication schemes. In [10] the authors used different cryptographic techniques, such as Merkle hash tree and identity-based signature schemes, to achieve immediate broadcast authentication and to minimize the computation and communication cost. The authors in [11] provide an ECC based solution to achieve authentication. Another ECC authentication scheme is proposed in [12]. The main disadvantage of these protocols is that PKC is not very efficient for use in WSNs due to its complexity and its high power requirement.

3. Tree Routing Overview

Tree-based Routing (TR) is an energy-efficient routing that is designed for lightweight networks. TR aims to reduce excessive messages among nodes and eliminate the overhead in path searching and table updating. The routing process in TR depends on the constructed tree among network nodes which is controlled by two parameters; tree depth and number of children. When the number of children increases/decreases, tree depth increases/decreases. After tree construction, an ID is assigned to each node. These logical IDs will be used as logical addresses for network nodes. Different control messages are used to control the tree

construction process. The structure of these messages varies according to systems' specification. But in general three main messages are used in any TR protocol. The first one is the *Association* message. Regardless how TR protocols refer to this message, it should be sent to all nodes in the neighborhood informing that the sender, usually called the parent, can accept children. The second message is the *AssociationReply*. This message is sent as a reply to the *Association* message to associate the node with the parent node. Finally, the third message is the *IDMessage* which is sent by the parent and contains the logical ID for the child node.

In general, nodes association process is started by the tree root, which could be the sink node or a network coordinator, by broadcasting an *Association* message to its neighbors. The steps of the association process are listed in **Table 1** and **Table 2** for the sender and the receiver, respectively. In **Fig. 1** an example of logical tree construction is illustrated where the numbers inside network nodes are nodes logical IDs. **Fig. 1-(a)** represents the physical distribution of network nodes, **Fig. 1-(b)** shows the logical tree among network nodes and in **Fig. 1-(c)** the tree logical view is shown.

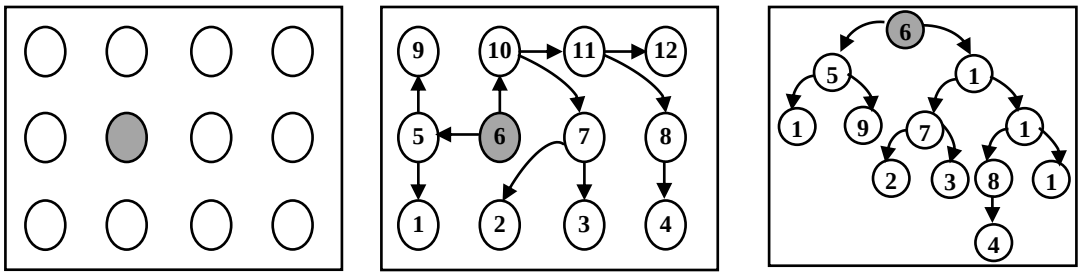
One of the drawbacks of TR protocols is path length; the deeper the sender node, the longer the path to the root. In addition to that, nodes failure is another important weakness in TR that causes nodes isolation.

Table 1. Nodes association process (sender side).

//Lm: tree depth	
//Cm: maximum number of children	
When any node get an ID, it will do the following:	
Step 1:	Broadcast *Association* message and wait for a reply.
Step 2:	When an *AssociationReply* message is received, Check Lm and Cm, if successful, then go to step 3 else go to step 4.
Step 3:	Send an *IDmessage* then go back to step 2.
Step 4:	Ignore the reply message
Step 5:	Exit

Table 2. Nodes association process (receiver side).

If the node does not have an ID, it will do the following:	
Step 1:	If an *Association* message is received then send an *AssociationReply* message.
Step 2:	If an IDmessage is received then go to step 3 otherwise go back to step 1.
Step 3:	Start the sender side process (Table 1).



(a) Physical distribution of network nodes.

(b) Logical tree among network nodes.

(c) Tree logical view.

Fig. 1. An example of logical tree construction.

In order to improve the weaknesses of TR protocols, many tree-based routing protocols have been proposed. Some of these protocols solve the problem of long paths by either proposing techniques that build two complementary trees rooted at the sink node with low average path length [13] or by utilizing neighbors' links in a company with parent-child links to find the shortest path to the sink node [14][15]. Alternatively, some protocols solve nodes failure problem by proposing fault tolerant routing protocols [16][17] that reconstruct the tree when a failure occurs.

In [14] and [15] Enhanced Tree Routing (ETR) and Improved Tree Routing (ImpTR) are proposed, respectively. These protocols, which are based on the tree routing protocol that is supported by IEEE 802.15.4 [18], improve the TR protocols by constructing neighbors' tables that are used to find the shortest path to the root. An addressing scheme is used to assign logical addresses to network nodes. In [16] Plus Tree routing protocol is proposed. This protocol aims to reduce the number of hops from the source to the destination by utilizing neighbors' links. In addition to that, it provides a solution for failure recovery. Plus tree protocol constructs the tree among network nodes based on TR association process. After constructing the tree, each node broadcasts its ID in order to build neighbors' tables. Another protocol that was proposed to solve the problems of TR protocol is Fuzzy-based Energy Aware Routing (FEAR) protocol that is proposed in [17]. This protocol provides energy-efficient solutions to find the shortest path and to solve nodes failure. It considers network limited energy and resources in its solutions.

4. SMTR

In this paper, a new security model for tree-based routing protocols is proposed. The objective is to build a security reference model that can be used to secure any tree-based routing protocol by applying suitable security techniques to ensure both correct and safe topology among network nodes and secure data transmission. In the next subsections, possible routing attacks and the suggested security requirements and techniques are discussed.

4.1 Tree Routing Attacks

In tree-based routing protocols control messages are used to manage nodes association and disassociation processes. When security techniques are not used, attackers can utilize these messages to affect the topology construction and exchange wrong topological information among nodes. Moreover, attackers can affect the process of data transmission by distributing false data or drop important packets. **Table 3** lists possible routing attacks and their consequences on tree-based routing process.

4.2 Security Requirements and Techniques

To protect the network from different routing attacks, some security prevention techniques must be applied to routing protocols. These techniques depend on the security requirements that should be achieved. Our concern in this paper is to establish a secure topology among network nodes and to secure the data transmission process.

To establish a secure topology and exclude adversary nodes, we need to make sure that all nodes that are participating in the construction phase are network sensors and not attackers. To ensure that, nodes authentication should be achieved. Another important requirement in order to ensure the distribution of correct topological information is data integrity. Attackers can modify important information carried in control messages allowing wrong topological

information to be exchanged among nodes. Thus, the proposed security framework will achieve both authentication and data integrity.

To achieve authentication and data integrity either Message Authentication Code (MAC) or Digital Signature (DS) techniques could be used. MAC algorithms are either hash based or block cipher based. On the other hand, DS uses Public Key Cryptography (PKC) to sign the message to be sent. In order to decide the best MAC or DS technique to be applied in the proposed security model, a study is conducted to evaluate different MAC and DS techniques to know their power efficiency. The evaluation is performed by applying the studied security techniques on TR protocols. These techniques are listed in **Table 4**. For block cipher based MAC, different ciphers could be used depending on the required level of security strength that should be achieved. In this paper some well-known ciphers are studied as well, as shown in **Table 5**. As illustrated in the table, block ciphers operate on different key and block sizes. For any block cipher, larger key size implies better security strength.

AES [19] is one of the most popular symmetric-key cryptography algorithms. It uses 4X4 array of bytes called the state array. Its main operations are substitution and permutation and it operates on a fixed block size of 128 bits and variable key size, 128, 192, or 256 bits, with 10, 12, and 14 rounds, respectively. RC5 [20] has a variable block size (32, 64, or 128 bits), number of rounds (0...255), and key size (0...2040 bits). The number of rounds does not depend on the key size, thus, the security strength of this algorithm can be determined by both the key size and the number of rounds. Unlike AES and RC5, Skipjack [21] uses 80-bit key size, 64-bit block size, and 32 rounds. The use of constant parameters reduces the flexibility of this algorithm. Finally, XXTEA [22] is the successor of XTEA and it was designed to correct flaws in the original Block Tiny Encryption Algorithm (TEA). It uses 128-bit key size and it is suitable to be used in resource constraint environments due to its low memory requirements.

Table 3. Tree-based Routing attacks and their consequences.

Routing Phase	Attack	Consequences
Nodes association and disassociation	1- Send a large number of fake control messages.	1.1 Overrun sensors' resources due to the cost of receiving, processing, and storing fake control messages. 1.2 sensors add the adversary node to their neighbors table.
	2- Eavesdrop on network control messages.	2.1 Adversary node knows network topology.
	3- Modify the contents of the network control messages.	3.1 Sensors store wrong topological information in their tables.
Data Transmission	1- Send fake data packets.	1.1 Affect the services provided by the sensor network by allowing wrong responses. 1.2 Allow the trigger of false alarms especially when fake critical data is sent. 1.3 Overrun sensors' resources due to the cost of forwarding, processing, and storing fake data packets.
	2- Eavesdrop on network data packets.	2.1 Access and read network data in an unauthorized way.
	3-Modify contents of the network data packets.	3.1 Affect the objectives of the sensor network by allowing wrong responses. 3.2 Allow the trigger of false alarms especially when critical data is modified.
	4- Drop data packets.	4.1 Prevent important data from being received and processed by the sink. 4.2 Affect the services provided by the sensor network.

Table 4. Studied security techniques.

	Security Technique	Main Process
Message Authentication Code Techniques	CBC-MAC	Block Cipher
	XMAC	Block Cipher
	CMAC	Block Cipher
	HMAC	Hash Function
Digital Signature Techniques	RSA	PKC
	ECDSA	PKC- based on Elliptic Curve Cryptography (ECC)

Table 5. Security strengths of the studied block ciphers.

Block cipher scheme	Block size (bit)	Key size (bit)	Security strength
AES	128	128	Secure for 10 rounds
RC5	32	128	Secure for more than 16 rounds
Skipjack	64	80	Currently considered unbreakable for 32 rounds
XXTEA	64	128	Secure for more than 6 rounds

CBC-MAC is a technique used for calculating MAC value based on a block cipher. The message is encrypted using the block cipher algorithm in CBC mode to create a chain of blocks. The MAC value, which will be added to the message, is the value resulted from the encryption of the last block. It uses two different keys one key is used by the block cipher algorithms (CBC) and the other for the MAC calculation [23]. In this way any change to any plaintext bit will cause a significant change in the final encrypted block that cannot be predicted without knowing the block cipher key. One variation of CBC-MAC is the XMAC. It operates with one key and supports variable-length messages. Another variation to CBC-MAC is the CMAC in which only one key is used for the computation. The key size for CBC-MAC, XMAC, and CMAC is $2K$, $K + 2n$, and K, respectively, where K is the key length of the underlying encryption algorithm and n is the block size of the cipher. On the other hand, HMAC does not base on block ciphers to calculate the MAC value, instead, it uses an iterative cryptographic hash function such as MD5 which divides the message into fixed-size blocks (e.g. 128 bits for MD5) and iterates over them with a compression function [23].

RSA [24] and ECDSA [25] are two well-known public key cryptography techniques that use two keys; private and public. The private key is used to sign the message while the public key is used to verify the signature. Generally, the security strength of PKC techniques is better than symmetric approaches, but they are more complex. In addition, some verification processes should be applied to verify the correctness of the public key.

4.3 SMTR Structure

The use of authentication and data integrity techniques requires that all nodes agree on key(s) before applying the security scheme. Regarding this, the following assumptions are considered:

- All required keys are preloaded into network sensors.
- All sensors are participating in the security verification process.

The proposed framework consists of two modules. The first module, which is illustrated in **Fig. 2-(a)**, is used during node association process and it aims to ensure secure topology and correct topological information among nodes. On the other hand, the second module, which is shown in **Fig. 2-(b)**, is used when all nodes are associated with network tree and are ready to

send data. This module aims to secure the data transmission process based on different factors that will be discussed later in this paper.

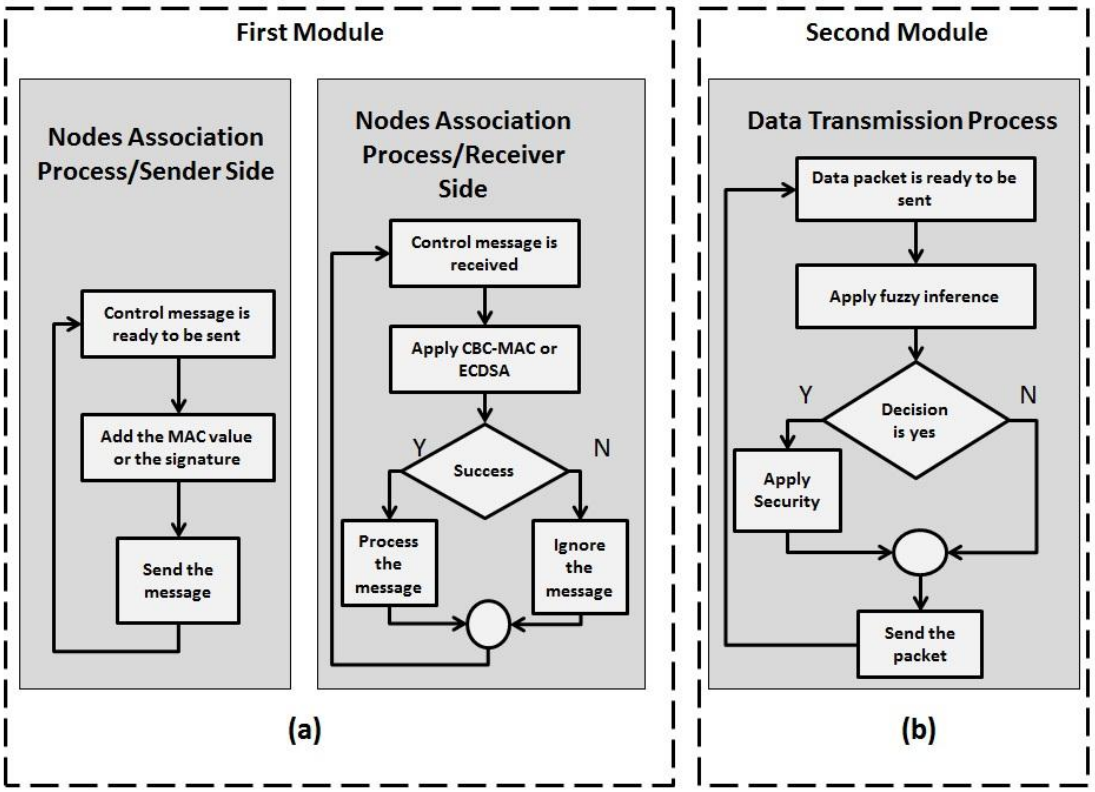


Fig. 2. SMTR Modules.

As illustrated in **Fig. 2**, in the second module, a fuzzy inference system will be used to decide whether to apply security techniques on the data packet or not. The two modules will be discussed in details in the following subsections.

4.3.1 First Security Module

This module should be used for all control messages in order to ensure secure tree architecture formation. During the tree construction or reconstruction, any control message should be either signed or embedded with a MAC value. When a sensor receives a control message, it should verify whether the message was sent by an authenticated node or not. If the sender is not authenticated, then the message should be ignored, otherwise adversary nodes will be treated as normal nodes and included in the constructed topology. Additionally, the receiver should verify if the message is received without any modifications. Modified messages should also be ignored since they may contain wrong topological information that will lead to unsafe and unsecure topology construction.

4.3.2 Second Security Module

In general, network sensors sense data and send it to the sink node. Unlike nodes association phase, this phase is performed periodically. Since some applications require short periods between data transmission, applying security on each data packet is not energy efficient. In

order to apply security during data transmission phase, a fuzzy inference system is used to decide whether to apply security techniques on a certain data packet or not. This decision depends on different parameters that will be discussed next. To reduce the consumed energy in the network, only the sender node will perform this module and intermediate nodes will only forward the data packet to the sink without any verification. The verification process will be performed at the sink node.

The fuzzy inference illustrated in **Fig. 3** has three inputs and one output. Based on mamdani fuzzy reasoning [26], the rules listed in **Table 6** are derived. The inputs to this system are Sender Energy (SE), Time since Last nodes Association process (TLA), and Data STatus (DST). SE has a higher priority among other parameters. That means when SE is low; the decision will be not to apply security regardless of the other two parameters. Moreover, when data is low critical, there is no need to apply security on the data packet.

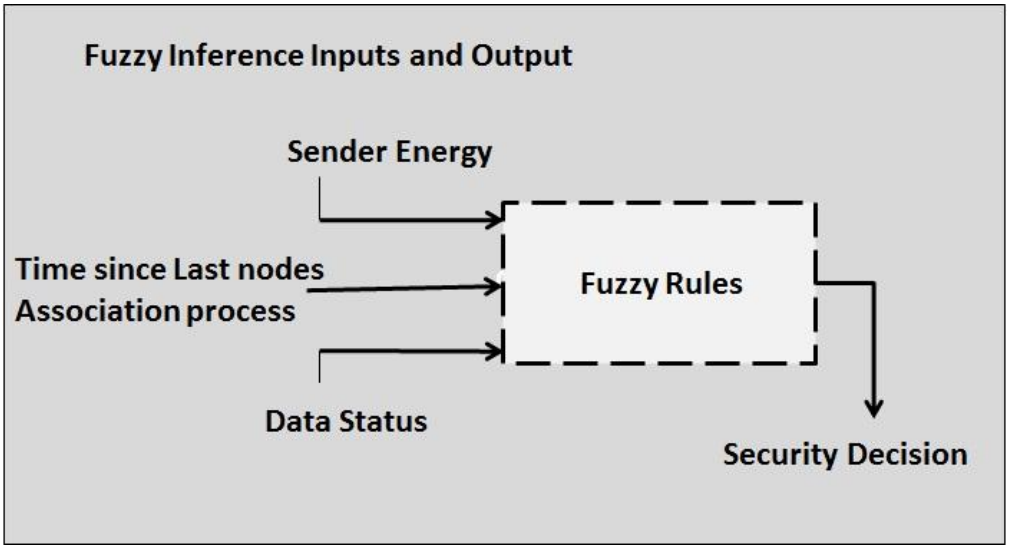


Fig. 3. Fuzzy inference structure.

Table 6. Fuzzy inference rules.

1	If (SE is Low) and (TLA is Short) and (DST is LowCritical) then (Decision is DoNotApply)
2	If (SE is Low) and (TLA is Medium) and (DST is LowCritical) then (Decision is DoNotApply)
3	If (SE is Low) and (TLA is Long) and (DST is LowCritical) then (Decision is DoNotApply)
4	If (SE is Low) and (TLA is Short) and (DST is HighCritical) then (Decision is DoNotApply)
5	If (SE is Low) and (TLA is Medium) and (DST is HighCritical) then (Decision is DoNotApply)
6	If (SE is Low) and (TLA is Long) and (DST is HighCritical) then (Decision is DoNotApply)
7	If (SE is Medium) and (TLA is Short) and (DST is LowCritical) then (Decision is DoNotApply)
8	If (SE is Medium) and (TLA is Medium) and (DST is LowCritical) then (Decision is DoNotApply)
9	If (SE is Medium) and (TLA is Long) and (DST is LowCritical) then (Decision is DoNotApply)
10	If (SE is Medium) and (TLA is Short) and (DST is HighCritical) then (Decision is Apply)
11	If (SE is Medium) and (TLA is Medium) and (DST is HighCritical) then (Decision is Apply)
12	If (SE is Medium) and (TLA is Long) and (DST is HighCritical) then (Decision is Apply)
13	If (SE is High) and (TLA is Short) and (DST is LowCritical) then (Decision is DoNotApply)
14	If (SE is High) and (TLA is Medium) and (DST is LowCritical) then (Decision is DoNotApply)
15	If (SE is High) and (TLA is Long) and (DST is LowCritical) then (Decision is DoNotApply)
16	If (SE is High) and (TLA is Short) and (DST is HighCritical) then (Decision is Apply)
17	If (SE is High) and (TLA is Medium) and (DST is HighCritical) then (Decision is Apply)
18	If (SE is High) and (TLA is Long) and (DST is HighCritical) then (Decision is Apply)

SE represents the residual amount of energy at the sender node. This input has three membership functions; low, medium, and high. The higher the amount of the sender energy, the better the chance for applying security technique on the data packet. TLA is used to indicate the time from the last association process. It has three membership functions; short, medium, and long. The shorter the time value, the lower the need for applying security techniques. This is because security is used in every association process, and if the association process is performed just before a short period of time, then all nodes in the topology will be authenticated and the topology is secure. Finally, DST is used to indicate how critical the sensed data is. If the data to be sent is critical, i.e. below or above a certain threshold (depending on the application), then the need for applying security on this data increases. This is used because applications usually concerns about securing critical data more than they concern about less critical data. By applying security on critical data, the correctness of this data is guaranteed. For example the amount of patient's blood pressure in medical applications is considered critical value when it increases above a specific threshold or decreases below another threshold. Caregivers will define the values of these thresholds based on her/his medical experience. The idea is to apply security only when blood pressure amount is critical because if attackers modify this value to normal one, then the system will not trigger any alarm to caregivers and the patient's status may be affected. On the other hand, if this value is normal and the attackers modify it to critical value then false alarms will be triggered to be handled by caregivers.

The output from the fuzzy inference system is the decision whether to apply security techniques on the current data packet or not. The membership functions for the fuzzy inference inputs and output are represented by either a trapezoidal or a triangular function. The trapezoidal four vertexes are (a,0), (b,1), (c,1) and (d,0), and the triangular three vertexes are (a,0), (b,1), and (c,0). The trapezoidal and triangular membership functions are represented in equations (1) and (2), respectively.

$$\mu(x,a,b,c,d)=\begin{cases}0 & x<a, x>d\\ \dfrac{x-a}{b-a} & a\le x\le b\\ 1 & b<x<c\\ \dfrac{d-x}{d-c} & c\le x\le d\end{cases} \tag{1}$$

$$\mu(x,a,b,c)=\begin{cases}0 & x<a, x>c\\ \dfrac{x-a}{b-a} & a\le x\le b\\ \dfrac{c-x}{c-b} & b\le x\le c\end{cases} \tag{2}$$

Based on the simulation experiments described in section 6, the values of a, b, c, and d for each membership function are tuned to give the optimal values that are shown in **Table 7**. It is worth mentioning that the values of a, b, c and d are not fixed and can be modified based on applications or services provided by WSNs. Note that all parameters values are mapped to values between 0 and 1 before applying the fuzzy inference system. For more illustration on how the fuzzy inference works, suppose that the inputs to the fuzzy inference system are: SE = 0.6, TLA = 0.4 and DST = 0.3 then rule 8 (from **Table 6**) will be activated since SE is medium,

TLA is also medium, and DST is low critical. In this case the output will be not to apply security on the current data packet.

Table 7. The values of a, b, c, and d for each fuzzy membership function.

Fuzzy Variable	Membership Function	Membership Function Type	Membership Function Parameter Values
SE	Low	Trapezoidal	a= 0, b = 0, c = 0.2, d= 0.4, x = the current value of SE
	Medium	Triangular	a= 0.3, b = 0.5, c = 0.7, x = the current value of SE
	High	Trapezoidal	a= 0.6, b = 0.8, c = 1, d = 1, x = the current value of SE
TLA	Short	Trapezoidal	a= 0, b = 0, c = 0.2, d= 0.4, x = the current value of TLA
	Medium	Triangular	a= 0.3, b = 0.5, c = 0.7, x = the current value of TLA
	Long	Trapezoidal	a= 0.6, b = 0.8, c = 1, d = 1, x = the current value of TLA
DST	Lowcritical	Trapezoidal	a= 0, b = 0, c = 0.3, d = 0.6, x = the current value of DST
	Highcritical	Trapezoidal	a= 0.4, b = 0.8, c = 1, d = 1, x = the current value of DST
Decision (Output)	DoNotApplySecurity	Trapezoidal	a= 0, b = 0, c = 0.3, d = 0.6, x = the output value
	ApplySecurity	Trapezoidal	a= 0.4, b = 0.8, c = 1, d = 1, x = the output value

5. SMTR Cost Analysis

In this section we will analyze the energy cost of the proposed security framework. Applying security schemes to achieve authentication and data integrity requires the sensor to perform local operations to verify the correctness of the message. This process costs the sensor some of its energy. In TR protocols, sending and receiving messages are the main energy consuming operations that are performed by all sensors, thus, most of the sensor energy is consumed by the communication operations. When applying security schemes, the local processing should also be considered in the energy consumption calculation. Therefore, sensor energy will be consumed through both communication and processing operations. **Table 8** lists all abbreviations that are used in the equations.

Table 8. List of abbreviations.

Abbreviation	Meaning
N	Number of nodes.
k	Message size in bits.
d	Distance between sender and receiver.
BC	Block Cost. Depends on the used security mechanisms.
BS	Block Size. Depends on the used security mechanisms.
AS_i	The size of i^{th} *Association* message.
ARS_i	The size of i^{th} *AssociationReply* message.
IDS_i	The size of i^{th} *IDmessage*.
ni	Number of neighbors for node i.
TCC	Tree Communication Cost.

5.1 Communication Cost Analysis

To measure the communication cost, both message size and sending distance should be known. According to [27] the communication cost for sending and receiving *k* bits message placed at distance *d* from the destination can be measured by equations (3) and (4).

$$\text{Sending\_Cost}(k,d) = \text{Eelec} \times k + \text{Eamp} \times kd^2 \quad (3)$$

$$\text{Receiving\_Cost}(k) = \text{Eelec} \times k \quad (4)$$

Where Eelec = 50 nJ/bit and Eamp = 100 pJ/bit/m^2

To measure the communication cost that is required to build the tree among network nodes, we need to know the total number of sent and received messages during this phase. According to the association process (illustrated in **Tables 1** and **2**, we have derived the required number of sent messages as $2 \times N + \sum_{i=1}^{n} n_i$ and the number of received messages as $N + 2 \times \sum_{i=1}^{n} n_i$. Thus, the communication power can be calculated according to equation (5). See **Table 9** for more illustration of these numbers.

$$TCC = Sending\_Cost(k,d) \times \left(2 \times N + \sum_{i=1}^{n} n_i\right) + \text{Re}ceiving\_Cost(k) \times \left(N + 2 \times \sum_{i=1}^{n} n_i\right) \quad (5)$$

Table 9. Estimated number of sent and received messages during node association process.

Message	Number of Sent Messages from Each Node	Number of Received Messages to Each Node
Association Messages	Each node sends one Association message, the total is N messages	Each node receives n_i Association Message, the total is
AssociationReply Message	Each node send AssociationReply to each Association, the total is $\sum_{i=1}^{n} n_i$	Each node expects to receive Replies from its neighbors. the total is $\sum_{i=1}^{n} n_i$
IDMessage	Each node receives one IDMessage. The total is N IDmessages	Each node receives only one IDmessage. The total is N ID messages
Total	$2 \times N + \sum_{i=1}^{n} n_i$	$N + 2 \times \sum_{i=1}^{n} n_i$

5.2 Processing Cost Analysis

As mentioned previously, applying security techniques costs the sensor some of its energy due to the processing cost. The cost of processing one control message is calculated by equation (6).

$$MessageCost = NumofBlocks \times BC \quad (6)$$

Where

$$NumofBlocks = \left\lceil \frac{k}{BS} \right\rceil$$

By knowing the number of messages that is exchanged among network nodes during the association process, we can measure the cost that is required to process these messages. Theorems 1 and 2 are used to find the processing cost for sending and receiving messages, respectively.

Theorem 1. In the proposed security framework (SMTR), the maximum amount of energy that is consumed by processing the sent messages during nodes association process is $\sum_{i=1}^{n}\left(\left\lceil \frac{AS_i}{BS}\right\rceil+\left\lceil \frac{IDS_i}{BS}\right\rceil\right)+\sum_{i=1}^{n}\left(n_i\times\left\lceil \frac{ARS_i}{BS}\right\rceil\right)\times BC.$

Proof. According to TR protocols, three control messages are sent during node association process, which are *Association*, *AssociationReply*, and *IDmessages*. The required number of *Association* messages is N. Based on this we have derived the number of blocks for all *Association* messages to be equal $\sum_{i=1}^{n} n_i\left(\left\lceil \frac{AS_i}{BS}\right\rceil\right)$. The same calculation is done for *AssociationReply* and *IDmessage* with $\sum_{i=1}^{n} n_i\left(n_i+\left\lceil \frac{ARS_i}{BS}\right\rceil\right)$ and $\sum_{i=1}^{n} n_i\left(\left\lceil \frac{IDS_i}{BS}\right\rceil\right)$ blocks, respectively. After finding the number of blocks for all control messages we use Equation (4) to find that the total cost is: $\sum_{i=1}^{n}\left(\left\lceil \frac{AS_i}{BS}\right\rceil+\left\lceil \frac{IDS_i}{BS}\right\rceil\right)+\sum_{i=1}^{n}\left(n_i\times\left\lceil \frac{ARS_i}{BS}\right\rceil\right)\times BC.$ □

Theorem 2. In the proposed security framework, the maximum amount of energy that is consumed by processing the received messages during nodes association process is $\sum_{i=1}^{n}\left(\left\lceil \frac{IDS_i}{BS}\right\rceil\right)+\sum_{i=1}^{n}\left(n_i\times\left\lceil \frac{AS_i}{BS}\right\rceil\times\left\lceil \frac{ARS_i}{BS}\right\rceil\right)\times BC.$

Proof. According to TR protocols, three control messages are received during node association process, which are *Association*, *AssociationReply*, and *IDmessage*. The required number of *Association* messages $\sum_{i=1}^{n} n_i$. Based on this, we derived the number of blocks for all *Association* messages to be equal to $\sum_{i=1}^{n} n_i\times\left\lceil \frac{AS_i}{BS}\right\rceil$. Same calculation is done for *AssociationReply* and *IDmessages* with $\sum_{i=1}^{n}\left(n_i\times\left\lceil \frac{ARS_i}{BS}\right\rceil\right)$ and $\sum_{i=1}^{n}\left\lceil \frac{IDS_i}{BS}\right\rceil$blocks, respectively. After finding the number of blocks for all control messages we use Equation (4) to find that the total cost is: $\left(\sum_{i=1}^{n}\left(\left\lceil \frac{IDS_i}{BS}\right\rceil\right)\right)+\left(\sum_{i=1}^{n}\left(n_i\times\left\lceil \frac{AS_i}{BS}\right\rceil\times\left\lceil \frac{ARS_i}{BS}\right\rceil\right)\right)\times BC.$ □

6. Security Framework Evaluation and Simulation Results

In this section the energy estimated cost for applying security techniques on TR protocols and the simulation results are discussed. This section also presents the evaluation for SMTR.

6.1 Security Techniques Evaluation

In this section the simulation results of the security techniques will be discussed. We use QualNet network simulator in our experiments. The simulation parameters are shown in **Table 10**. We have evaluated the efficiency of different security techniques by applying them to the TR protocols based on the energy requirements illustrated in **Table 11**.

6.1.1 Energy Cost Estimation for Security Requirements

As discussed previously, different MAC algorithms are evaluated to know their power efficiency by applying them to TR protocols. The performance of cipher based MAC techniques depends on the underlying block cipher that is used to calculate the MAC value. Many previous works evaluated the performance of block ciphers [23], digital signatures [28], and MAC techniques [23]. In this paper, based on the results in [23][28] we have derived the energy cost requirements for the comparable techniques when applying them to TR protocols on both MicaZ and TelosB sensor motes. MicaZ and TelosB are two known sensor motes that differ in their memory size and energy efficiency. MicaZ motes have 4 KB of RAM, 128 KB of ROM and TelosB motes have 10 KB of RAM, 48 KB ROM. In terms of energy efficiency, TelosB motes are more efficient than MicaZ [23]. Crossbow Technology, Inc. is a well-known in producing such sensor motes. It is one of the first, leading suppliers of low-cost, smart-sensor technology to military and tracking systems. For up-to-date information and data sheets about their product lines, the reader can refer to their official website [29].

Table 10. Simulation parameters.

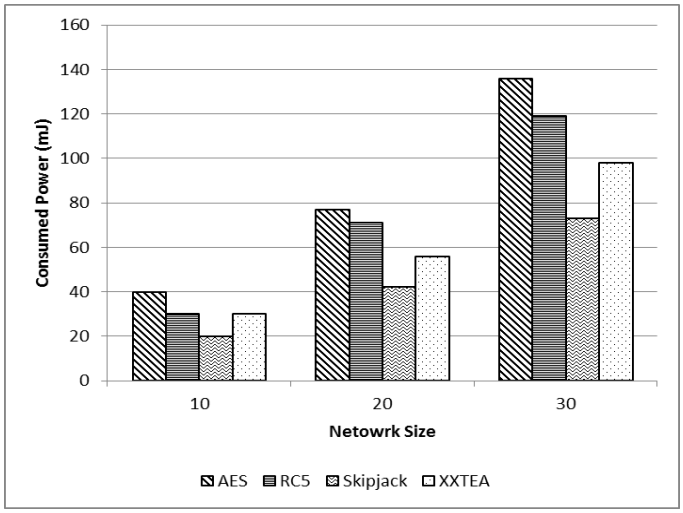
Simulation Parameter	Value
Network Size	Up to 30 nodes
Terrain Area (m^2)	1500 × 1500
Mobility	None
Radio Range (m)	250
Number of Sinks	1
Initial Energy (J)	1000

Table 11. Security techniques energy cost estimation.

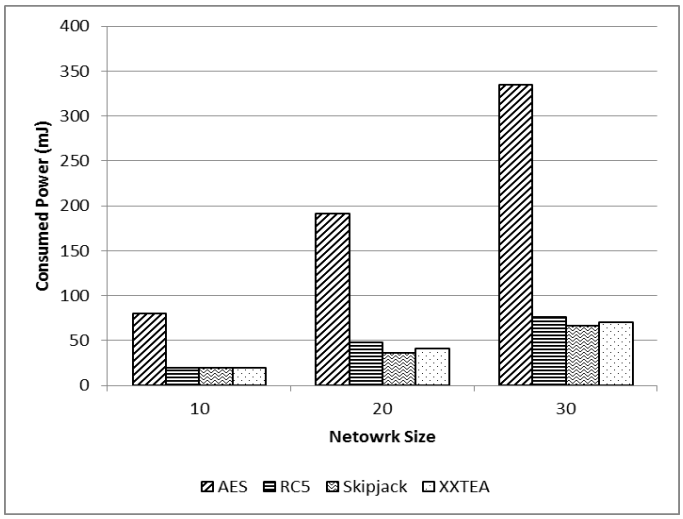
	Security technique	Energy per 128 bit data block (µJ)							
		MicaZ				TelosB			
Block Cipher Technique	AES	146.6				425.49			
	RC5	137.92				58.26			
	Skipjack	27.58				13.3			
	XXTEA	124.64				38.7			
MAC Techniques		*AES*	*RC5*	*Skipjack*	*XXTEA*	*AES*	*RC5*	*Skipjack*	*XXTEA*
	CBC-MAC	160.39	178.78	123.61	172.14	112.2	98.45	75.97	88.97
	XMAC	264.59	282.98	227.81	276.34	176.44	162.69	140.21	152.91
	XMACHMAC	387.19	405.58	350.41	398.94	250.39	236.64	214.16	226.86
	HMAC	278.39				57.37			
Digital Signature Techniques		*Sign (mJ)*		*Verify (mJ)*		*Sign (mJ)*		*Verify (mJ)*	
	RSA-1024	359.87		14.05		68.97		2.7	
	ECDSA-160	26.96		53.42		6.26		12.41	

6.1.2 Block Ciphers Evaluation

In this section the results of block ciphers evaluation will be illustrated. Different block ciphers are studied which are AES, RC5, Skipjack, and XXTEA on MicaZ and TelosB sensor motes. The evaluation is done by applying each scheme on TR protocols and then measuring the consumed energy in *mJ* using different network sizes. **Fig. 4-(a)** and **(b)** illustrate the energy that is consumed by the encryption and decryption operations for each block cipher on MicaZ and TelosB motes, respectively. As illustrated in the figures, the consumed energy increases as the number of nodes increases. Moreover, block cipher schemes have a better energy saving when operate on TelosB mote except for AES. In both motes AES is the most energy consuming scheme while skipjack has the best energy saving.



(a) MicaZ mote.

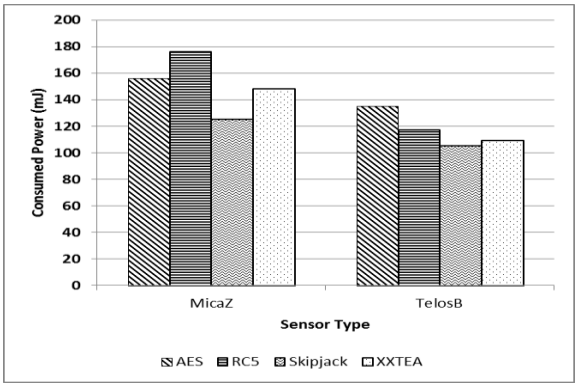


(b) TelosB mote.

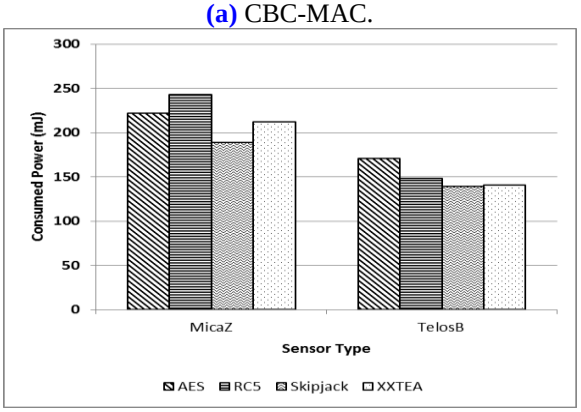
Fig. 4. Different block ciphers in terms of the consumed energy against different network sizes.

6.1.3 MAC Techniques Evaluation

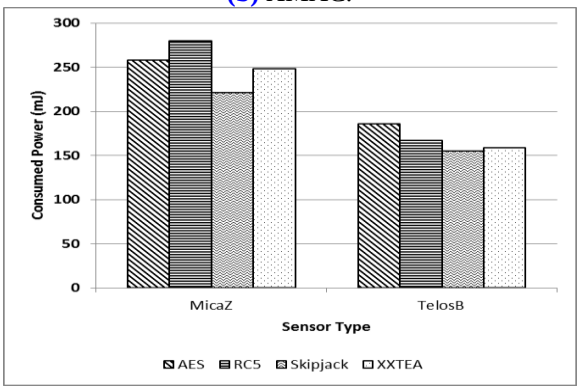
Four MAC techniques are studied which are CBC-MAC, XMAC, CMAC, and HMAC. The first three techniques are based on block ciphers to calculate the MAC value. We evaluate each one of them by applying it to TR protocols using the four studied block ciphers. The results are shown in **Fig. 5-(a)**, **(b)**, and **(c)**, respectively. As illustrated in the figures, CBC-MAC is more efficient than the other techniques and it operates better when skipjack block cipher is used. On the other hand, HMAC technique does not depend on block cipher instead it uses hash function to calculate the MAC value. The energy that is consumed by HMAC on MicaZ and TelosB is illustrated in **Fig. 6**.



(a) CBC-MAC.



(b) XMAC.



(c) CMAC.

Fig. 5. The consumed energy using different block ciphers.

6.1.4 Digital Signature Techniques Evaluation

Two DS schemes based on PKC are evaluated in this paper which are RSA and ECDSA. The results show that ECDSA is more efficient than RSA on both MicaZ and TelosB sensor motes since it based on Elliptic Curve Cryptography (ECC) that is less complex than other PKC schemes. The results are shown in **Fig. 7**.

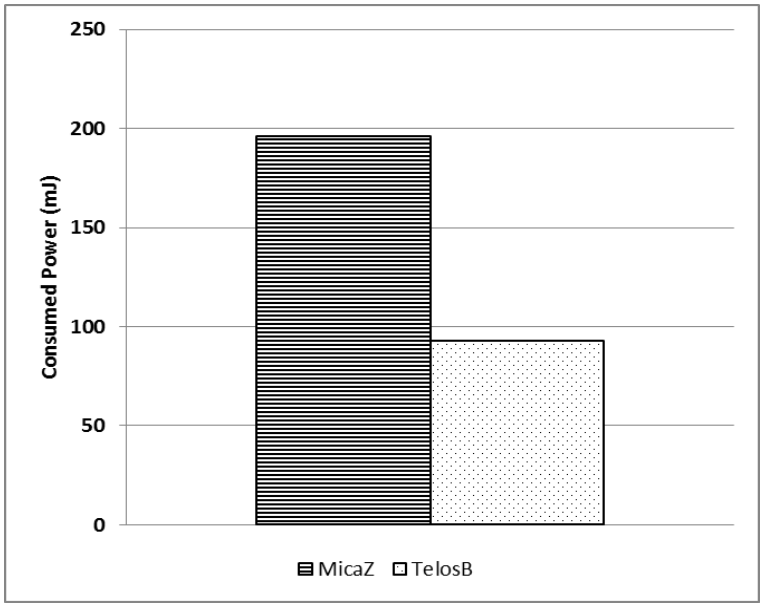


Fig. 6. The consumed energy by HMAC scheme using different sensor motes.

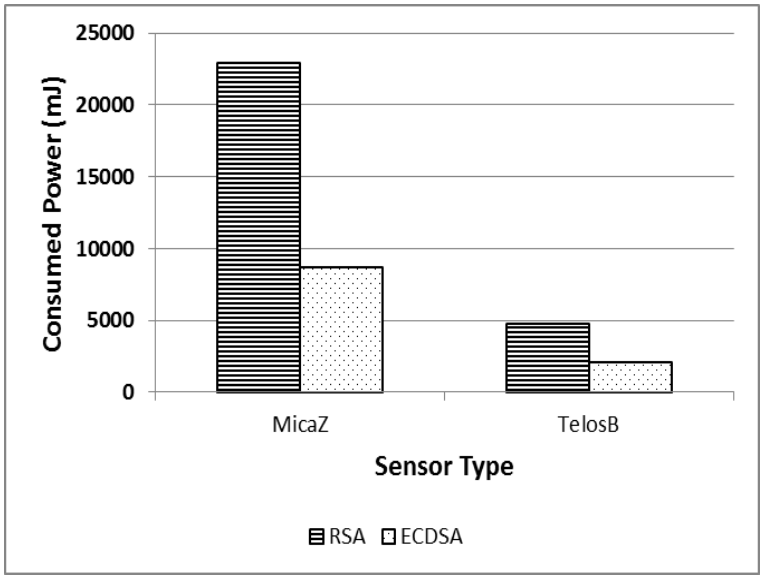
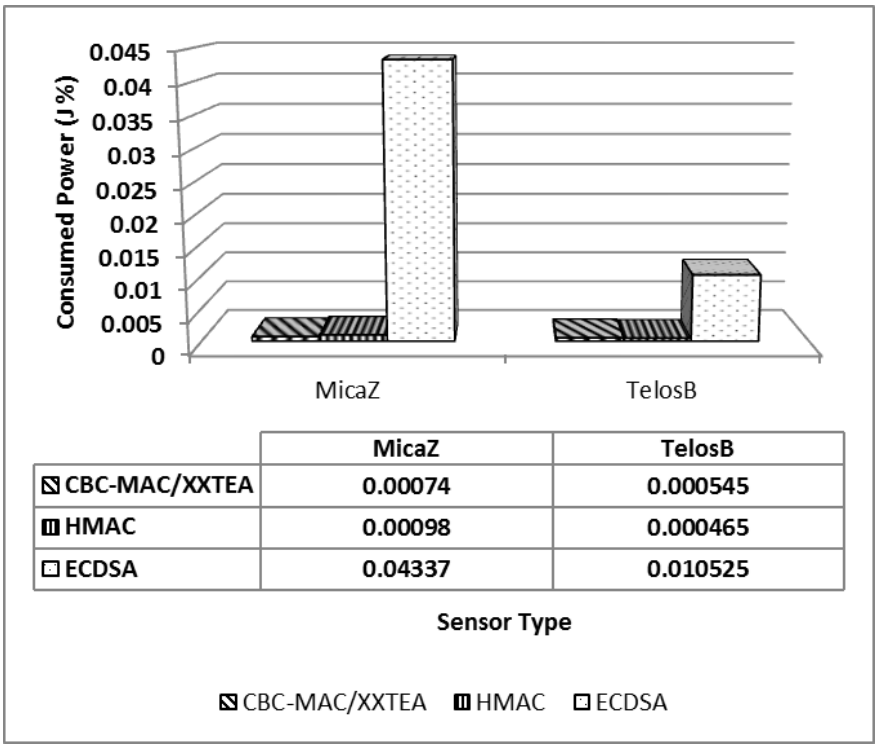


Fig. 7. Comparison between **DS** schemes in terms of consumed energy on different sensor motes.

6.2 SMTR Evaluation and Simulation Results

This section evaluates the two modules of SMTR and discusses the simulation results. To evaluate the first module (tree construction), we applied both MAC and DS techniques on different sensor motes. The results of comparing MAC and DS techniques are illustrated in **Fig. 8**. In our comparison we have selected one scheme from each category of the studied MAC and DS schemes. For block cipher based MAC schemes, CBC-MAC/XXTEA has been chosen since it has less energy consumption than AES and RC5 and better security strength than skipjack scheme (128-bit key size vs. 80-bit key size). In addition, we have selected HMAC and ECDSA. Generally, PKC schemes are not recommended for use in WSNs since they are based on asymmetric approaches that are more complex to be implemented than symmetric based ones. Results show that HMAC schemes cost the network about 0.000465% of its energy when is consumed on TelosB mote whereas when ECDSA is used, about 0.010525% of the network energy is consumed on the same sensor mote. The exact results are shown as a table below the figure for easy reference.

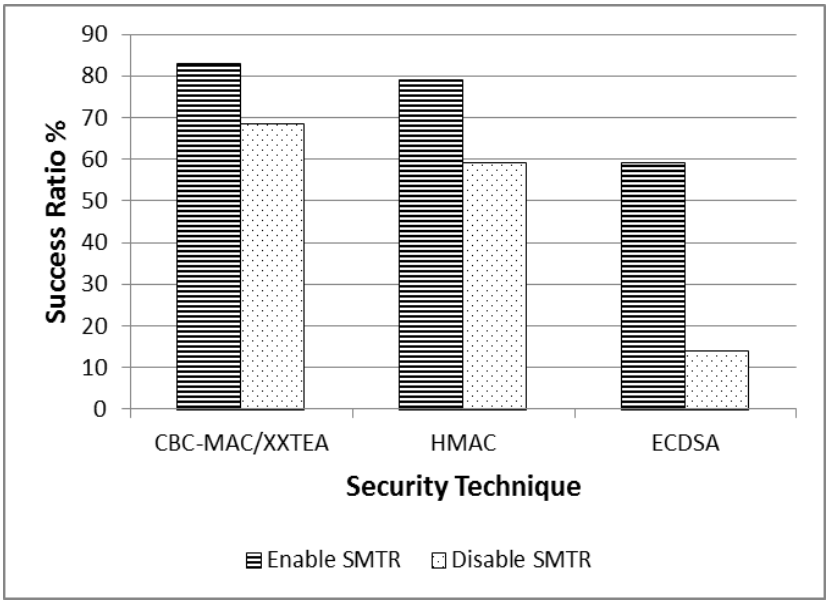


	MicaZ	TelosB
CBC-MAC/XXTEA	0.00074	0.000545
HMAC	0.00098	0.000465
ECDSA	0.04337	0.010525

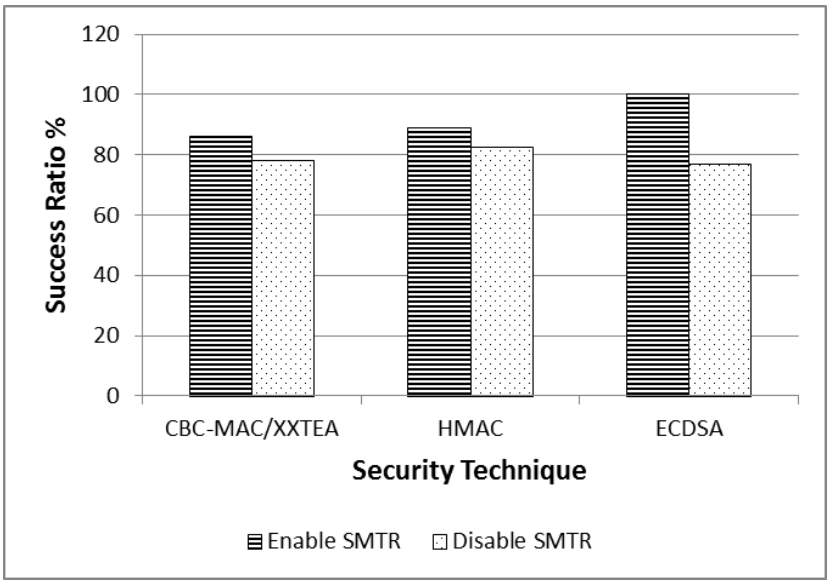
Fig. 8. Comparison between MAC and DS techniques during the first module (tree construction) of SMTR on different sensor motes.

Fig. 9 compares between different security techniques in terms of success ratio when SMTR second module is either enabled or disabled. Success ratio is defined as the percentage of successfully delivered data packets. In case of using MicaZ, **Fig. 9-(a)** shows that enabling the SMTR second module improves the success ratio by 14.5%, 20%, and 45% when

CBC-MAC/XXTEA, HMAC, and ECDSA security technics are used, respectively. From **Fig. 9-(b)**, when TelosB is used, it can be noticed that the improvement is 8%, 6.5%, and 23% with the use of CBC-MAC/XXTEA, HMAC, and ECDSA, respectively.



(a) MicaZ mote.



(b) TelosB mote.

Fig. 9. A comparison between different security techniques in terms of the success ratio when SMTR second module is enabled/disabled.

Fig. 10 shows the differences in the improvement of success ratio when MicaZ or TelosB are used. As shown in the figure, MicaZ is superior to TelosB. MicaZ improves the success ratio over TelosB by 6.5%, 13.5%, and 22% when CBC-MAC/XXTEA, HMAC, and ECDSA are used, respectively. **Fig. 11** compares between different security techniques in terms of network life time when SMTR second module is either enabled or disabled. Network life time is the time elapsed from the moment the network started its operations and until the first network sensor ran out of energy. Enabling the SMTR second module increases the network life time when both MicaZ and TelosB are used as shown in **Fig. 11-(a)** and **(b),** respectively. The improvements in success ratio and network life time is due to the use of fuzzy inference system to decide whether to apply security techniques on the data packet or not as discussed earlier is section 4.3.2. That means not applying security techniques to each data packet will save the sensors' energy, prolong the network life time and the sensors' abilities to send more data packet.

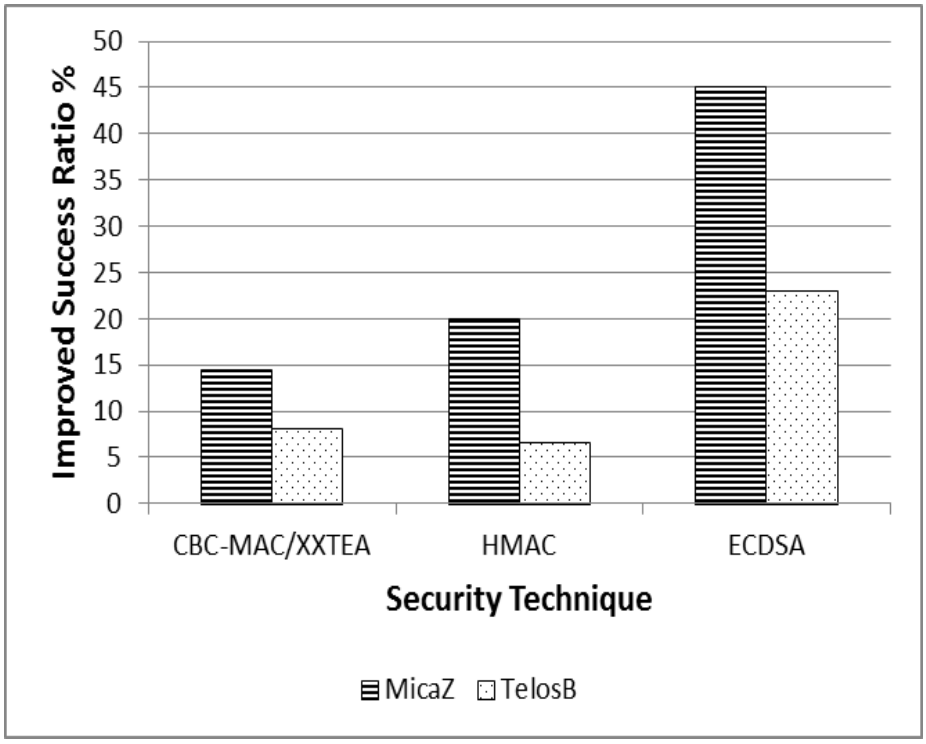
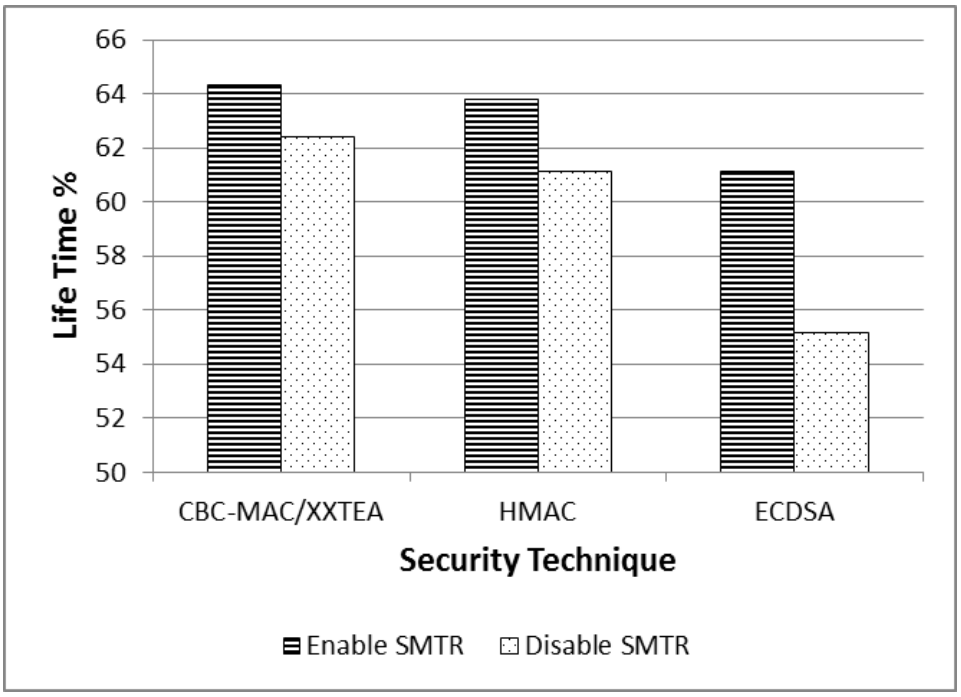
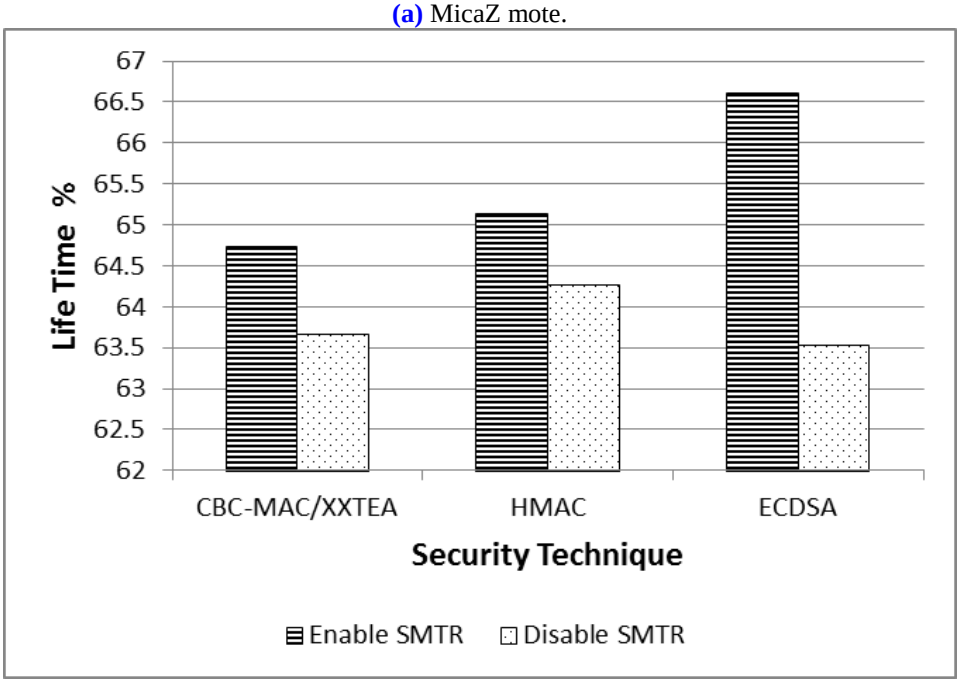


Fig. 10. Differences in improvement of success ratio between MicaZ and TelosB motes when SMTR second module is enabled.



(a) MicaZ mote.



(b) TelosB mote.

Fig. 11. A comparison between different security techniques in terms of the network life time when SMTR second module is enabled/disabled.

7. Conclusion

The paper has proposed an energy-efficient Security Model for Tree-based Routing protocols (SMTR) that can be used to secure any tree-based routing protocol. Moreover, we have studied the impact of routing attacks on both topology construction and data transmission process. In addition, we evaluate different MAC and DS techniques to be used by the proposed model. The results showed that using MAC techniques is more efficient in terms of energy saving than DS techniques since they are based on symmetric approaches. Also, the simulation experiments showed that enabling SMTR, improves the energy saving, data packet delivery success ratio and prolongs the network life time when either MicaZ or TelosB motes are used. The use of intelligent system to decide whether to apply security techniques on each data packet, leads to such improvements. As future work, we will build energy efficient Intrusion Detection System (IDS) to protect the network from compromised nodes. Consequently, the security model will protect the network from internal as well as external attacks.

References

[1] M. Abuhelaleh, T. Mismar and A. Abuzneid, "Armor-leach – energy efficient, secure wireless networks communication," in *Proc. of 17th International Conference on Computer Communications and Networks*, St. Thomas, Aug.2008. Article (CrossRef Link)

[2] E. Klaoudatou, E. Konstantinou, G. Kambourakis and S. Gritzalis, "Clustering oriented architectures in medical sensor environments," in *Proc. of Third International Conference on Availability, Reliability and Security*, pp.929 -934, Mar.2008. Article (CrossRef Link)

[3] M.R. Kanjee, K. Divi and L. Hong. "A Physiological Authentication Scheme in Secure Healthcare Sensor Networks," in *Proc. of 7th Annual IEEE Communications Society Conference on Sensor Mesh and Ad Hoc Communications and Networks*, Jun.2010. Article (CrossRef Link)

[4] R. Mukesh, A. Damodaram and V. S. Bharathi, "Energy Efficient Security Architecture for Wireless BioMedical Sensor Networks," *International Journal of Computer Science and Information Security*, vol.6, no.1, pp.116 -122, 2009. Article (CrossRef Link)

[5] T. Dimitriou and K. Ioannis, "Security issues in biomedical wireless sensor networks," in *Proc. of First International Symposium on Applied Sciences on Biomedical and Communication Technologies*, Oct.2008. Article (CrossRef Link)

[6] R. Söderlund, *Energy Efficient Authentication in Wireless Sensor Network*. Ph.D. Thesis, 2006. Article (CrossRef Link)

[7] A.-S. Pathan and C. Hong, "A secure energy-efficient routing protocol for WSN," In *Parallel and Distributed Processing and Applications*, pp.407-418, 2007. Article (CrossRef Link)

[8] A. Papadimitriou, F. Le Fessant, A. Viana and C. Sengul, "Cryptographic protocols to fight sinkhole attacks on tree-based routing in wireless sensor networks," in *Proc. of 5th IEEE Workshop on Secure Network Protocols*, pp.43-48, Oct.2009. Article (CrossRef Link)

[9] R. Soderlund, S. Svensson and T. Lennvall, "Energy efficient authentication in wireless sensor networks," in *Proc. of IEEE Conference on Emerging Technologies and Factory Automation*, pp.1412 -1416, Sep.2007. Article (CrossRef Link)

[10] K. Ren, W. Lou, K. Zeng and P. Moran, "On broadcast authentication in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol.6, no.11, pp.4136-4144, Nov.2007. Article (CrossRef Link)

[11] H.-L.Yeh, T.-H. Chen, P.-C. Liu, T.-H. Kim and H.-W. Wei, "A secured authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors*, vol.11, no.5, pp.4767-4779, May.2011. Article (CrossRef Link)

[12] S. Gupta, H. Verma and A. Sangal, "Authentication protocol for wireless sensor networks," *World Academy of Science, Engineering and Technology*, 66, pp.643-649, 2010. Article (CrossRef Link)

[13] L. Liu, Z. Ling and Y. Zuo, "Low-delay Node-disjoint Multi-path Routing using Complementary Trees for Industrial Wireless Sensor Networks," *KSII Transactions on Internet and Information Systems*, vol.5, no.11, pp.2052-2067, Nov.2011. Article (CrossRef Link)

[14] M. Al-Harbawi, M. Rasid and N. Noordin, "Improved Tree Routing (ImpTR) Protocol For ZigBee Network," *International Journal of Computer Science and Network Security*, vol.9, no.10, pp.146-152, Oct.2009. Article (CrossRef Link)

[15] W. Qiu, E. Skafidas and P. Hao, P. "Enhanced tree routing for wireless sensor networks," *Ad Hoc Networks*, vol.7, no.3, pp.638 – 650, May.2009. Article (CrossRef Link)

[16] Y. Park, E.-S. Jung, "Plus-tree: A routing protocol for wireless sensor networks," In *Advances in Hybrid Information Technology*, 2007. Article (CrossRef Link)

[17] I. Almomani and M. Saadeh, M. "FEAR: Fuzzy-Based Energy Aware Routing Protocol for Wireless Sensor Networks," *International Journal of Communications, Network and System Sciences*, vol.4, no.6, pp.403-415, Jun.2011. Article (CrossRef Link)

[18] IEEE. ZigBee Specification Version 1.0, ZigBee Alliance, 2005.

[19] NIST, the National Institute of Standards and Technology. Federal Information Processing Standards Publication-Announcing the ADVANCED ENCRYPTION STANDARD (AES), 2001. Article (CrossRef Link)

[20] Rivest, R. L. *The RC5 Encryption Algorithm*. Springer-Verlag, pp.86-96, 1995. Article (CrossRef Link)

[21] NIST, The National Institute of Standards and Technology, Skipjack and KEA algorithms specifications, version 2 1998. Article (CrossRef Link)

[22] D. Wheeler and R. Needham. *Correction to XTEA*. Cambridge University, 1998.

[23] J. Lee, K. Kapitanova and S. H. Son, "The price of security in wireless sensor networks," *Computer Networks*, vol.54, no.17, pp.2967 – 2978, Dec.2010. Article (CrossRef Link)

[24] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems" *Communication ACM*, vol.21, no.2, pp.120-126, Feb.1978. Article (CrossRef Link)

[25] D. Johnson, A. Menezes and S. Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," *International Journal of Information Security*, vol.1, no.1, pp.1, 36-63, Aug.2001. Article (CrossRef Link)

[26] E. Mamdani, "Application of fuzzy logic to approximate reasoning using linguistic synthesis," *IEEE Transactions on Computers*, vol.C-26, no. 2, pp.1182 -1191, 1977. Article (CrossRef Link)

[27] W. Heinzelman, A. Sinha, A. Wang and A. Chandrakasan, "Energy-scalable algorithms and protocols for wireless microsensor networks," in *Proc. of the 2000 IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '00)*, pp.3722-3725, Jun.2000. Article (CrossRef Link)

[28] P. Trakadas, T. Zahariadis, H. Leligou, S. Voliotis and K. Papadopoulos, "Analyzing energy and time overhead of security mechanisms in wireless sensor networks," in *Proc. of the 15th International Conference on Systems, Signals and Image Processing*, pp.137 -140, Jun.2008. Article (CrossRef Link)

[29] Crossbow Technology, Inc., http://www.xbow.com/.

Iman Musa Almomani received her B.Sc. degree in Computer Science from UAE University (UAE), M.Sc. degree in Computer Science from the University of Jordan (Jordan). Iman then worked at the University of Jordan as a Lecturer. After that she got her Ph.D. degree from De Montfort University, UK, in 2007. She is currently an assistant professor in the Computer Science Department in King Abdullah II School for Information Technology at the University of Jordan. Her research interests include wireless mobile ad hoc networks (WMANETs), Wireless Sensor Networks (WSNs) and security issues in wireless networks. Iman is in the organizing and technical committees for a number of local and international conferences. Also, she serves as a reviewer in a number of local and International Journals. Iman is also a member of IEEE and IEEE Women in Engineering.

Maha K. Saadeh obtained her B.Sc. degree in computer science from the University of Jordan, Amman, Jordan in 2009. She worked as research and teaching assistant at the computer science department, The University of Jordan from September 2009 to September 2010. Then she received her M.Sc. degree from the same university in 2011. She has a number of publications in a number of local and international journals and conferences. Her research interests are: Wireless networks, network security, and robotics.