Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 159 (2019) 803–813

Procedia Computer Science

www.elsevier.com/locate/procedia

23rd International Conference on Knowledge-Based and Intelligent Information & Engineering Systems

Improvement of Watermarking-LEACH Algorithm Based on Trust for Wireless Sensor Networks

Nejla Rouissi[a], Hamza Gharsellaoui[b,c,d,e,], Sadok Bouamama[a,f]

[a]National School of Computer Science (ENSI), Manouba University, Tunisia
[b]School of Intelligent Systems Science and Engineering, Jinan University (Zhuhai Campus), Zhuhai 519070, China
[c]National Engineering School of Carthage (ENICarthage), Carthage University, Tunisia
[d]LISI-INSAT Laboratory, National Institute of Applied Sciences and Technology (INSAT), Carthage University, Tunisia
[e]Khurmah University College (KUC), Taif University, KSA
[f]Higher College of Technology (DMC), Dubai, United Arab Emirates

Abstract

Wireless sensor networks (WSNs) consists of a large number of sensor nodes to monitor physical or environmental conditions. Each sensor node has specific tasks to do with its neighbours. On the other hand, if node does not perform it, it is considered as misbehaviour node and often interrupt the normal functionality of a WSN. In order to keep functional WSNs, it is necessary to identify the misbehaviour of the node, which will save the network from internal attacks. So, an effective security mechanism is essential. The work presented in this paper is concerned with introduced trust management based Watermarking-LEACH to prevent at the same time internal and external attacks. This leads to introduce a new trust model into Watermarking-LEACH schema to infer the total trust and security with the energy-efficiency. To this end, the implementation and simulation of T-W-LEACH approach is done with the MATLAB tool simulator and the evaluation of security and energy is made to perform a comparative with TBE-LEACH a Trust based energy efficient routing in LEACH for wireless sensor networks.

Keywords: Wireless Sensor Networks; Trust; Integrity; Falsification; Internal Attacks; Energy-Efficiency; MATLAB; Watermarking; External Attacks.

[1] Corresponding author. Tel.: +216-93-740-959.
E-mail address: rouissi.nejla@gmail.com

[2] Corresponding author. Tel.: +9665-56207-198.
E-mail address: gharsellaoui.hamza@gmail.com

[3] Corresponding author. email.: Sbouamama@hct.ac.ae.
E-mail address: Sadok.bouamama@ensi.rnu.tn

1877-0509
10.1016/j.procs.2019.09.239

1. INTRODUCTION

In wireless sensor networks the nodes are distributed to act specific tasks, monitor and record physical condition of the environment. If sensor node does not perform a normal behavior, this means a presence of misbehaviour node. So, these misbehaving nodes play a major role to decide the quality of service in WSNs. In order not to disrupt the operation of WSNs, it is necessary to identify the misbehaviour of the node, which will save the network from internal attacks. Besides, internal attacks cause serious damage to WSNs [1]. In this case, internal attacks are found in almost every layer, the internal node is compromised to the attacker due to some weakness in system but the external attack is performed by some external entities aiming at deteriorating the WSNs functionality. So, the detection of internal attack is more difficult than external attacks because the internal attacks can have partial keys of security mechanism with them and they are having trust of other sensor nodes. Although, the external attack are not having access to rules of security mechanism or cryptographic keys as they are not from the internal network [13]. So, an effective security mechanism is essential. However, the traditional security techniques used in traditional networks cannot be efficiently applied to WSNs directly due to sensors constraints. Therefore, the developpement of an efficient security mechanism to protect WSNs from internal attacks becomes a challenging task [14], [15].

Various cluster based protocols are proposed for WSN like LEACH [16] an hierarchical routing protocol special for WSN. Many researchers have proposed many improved algorithms based on LEACH [16], such as VLEACH [17], BN-LEACH [19], TBE-LEACH [8], these algorithms have much improvements on efficiency of energy in certain extent [18], but are vulnerable to internal or external attack.

So, we will extend the idea of the Watermarking-LEACH [5], that achieves data integrity against the data falsification. It is the first schema that attempts to add security based on watermarking to LEACH routing protocol. While, internal WSN nodes that act selfishly or maliciously are considered as internal attacks. This leads to introduce a new trust models into Watermarking-LEACH schema to infer the total trust and security also with the energy-efficiency. The work presented in this paper is concerned with introduced trust management based Watermarking-LEACH to prevent at the same time internal and external attacks.

To this end, the implementation and simulation of T-W-LEACH approach is done with the MATLAB tool simulator and the evaluation of security and energy is made to perform a comparative with TBE-LEACH a Trust based energy efficient routing in LEACH for wireless sensor network. This paper demonstrated high reliability and shows calculation of trust for nodes, trusted cluster head selection, secure routing and watermarking construction and extraction.
The remainder of this paper is organized as follows. In background Section, some preliminaries and concepts used in this approach are reviewed. Section III presents the proposed T-W-LEACH scheme. Section IV presents the experimentation steps and results. Finally, section V concludes the paper work.

1.1. BACKGROUND

This section present a brief description of some basic concepts used in literature to help understanding the contribution of the paper.

1.1.1. Internal attacks

The internal attack is considered when a legitimate node of the network acts abnormally or illicitly it. It uses the compromised node to attack the network which can destroy or disrupt the network easily. An adversary by physically capturing the node and reading its memory can obtain its key material and forge network messages. Having access to legitimate keys can give the attacker the ability to launch several kinds of attacks, such as false data injection and selective reporting, without easily being detected [9], [10].

1.1.2. External attacks

This attack is defined as the attack performed by a node that does not belong to the network. Obviously, the attacker node does not have any internal information about the network such as cryptographic information [11].

1.1.3. Digital Watermarking Technique

Digital watermarking may be used to verify data integrity or authenticity in WSNs. This method aims to protect the digital rights and embeds the pertinent data. So, watermarking data is directly associated with sensor data. Redundant space of the data is used to store the digital watermarking data. The generation and embedding of watermarking data is done at source sensor nodes, although, the extraction and its verification are maked at base station [6], [7].

1.1.4. LEACH Protocol Overview: LEACH - Low Energy Adaptive Clustering Hierarchy

LEACH Protocol is an hierarchical clustering-based routing protocol where each number of clusters is formed and each cluster has a cluster-head. Cluster head collects the data from sensor nodes to communicate directly with the base station. It is self-organizing and adaptive clustering. LEACH utilizes randomized rotation of local cluster base stations (cluster-heads) to evenly distribute the energy load among the sensors in the network, operations are broken into rounds, each round is made on two phases: Setup Phase and Steady Phase.

Phases of leach protocol are as follows:

Setup phase

In the setup phase, the main goal is to select the cluster head for each of the cluster by choosing the sensor node with maximum energy [21].

Setup phase has three fundamental steps:

1. Cluster head advertisement;
2. Cluster setup;
3. Creation of transmission schedule;

During the first step cluster head sends the advertisement packet to inform the cluster nodes that they have become a cluster determined by the following equation:

$$\mathbf{t(n)} = \begin{cases} \frac{p}{1-p*(r \bmod \frac{1}{p})} \; if \quad n \in G, \\ 0 \; if \quad n \notin G. \end{cases} \tag{1}$$

where T (n) is the threshold, P is the desired percentage of cluster head nodes in all sensors, r is the current round number, and G is the set of nodes not cluster head in the previous 1/p round. Node becomes cluster head for the current round if the number is less than threshold T (n). Once node is elected as a cluster head then it cannot become cluster head again until all the nodes of the cluster have become cluster head once [5], [21].

In the second step, non-cluster head nodes receive the cluster head advertisement and then send join request to the cluster head informing that they are members under that cluster head.

In third step, each cluster head creates a transmission schedule for the member nodes of their cluster. TDMA schedule is created according to the number of nodes in the cluster. Each node then transmits its data in the allocated time schedule [21].

Steady phase

In steady phase, cluster nodes send their data to the cluster head. The member sensors in each cluster can communicate only with the cluster head via a single hop transmission. Cluster head aggregates all the collected data and forwards data to the base station directly or via other cluster head. After predefined time, the network again goes back to the set-up phase.

Various secure improvements are done on LEACH protocol using cryptography. Although management of cryptographic keys in WSNs certainly drives many issues because they demand extensive use of resources, So, key storage is a challenging issue in sensor networks which still demands suitable solutions. Thus, we present a novel version of LEACH Based on Watermarking for WSNs because in our approach the watermarking information is directly embedded into the redundant space of the data. It does not occupy additional storage space such like cryptography algorithms.

For more details about watermarking-LEACH Protocol you can see [5],[20].

1.1.5. Trust Concept

Trust in wireless sensor network can be defined in various ways. According to [3] trust is the degree of reliability about other node for performing certain action by keeping track of all past transaction or interactions with nodes by direct or indirect observation. Trust can also be defined as the level of confidence that one node about other node to get assigned work done within some time. This level of confidence is calculated by one node about other node based on past interaction or transaction history. This trust value depends on time and it can decrease or increase according to evidences available from direct observations or recommendations from trusted neighbouring nodes. To calculate the trust we need some evaluation technique based on some mathematical model. Trust management in wireless sensor network is essential as these can be used in taking decisions about different activities of network [4]. As wireless sensor networks are being used for various applications, these have different needs of security. Working principle of WSN totally depends on cooperativeness and trusting nature of sensor nodes. That is why establishment of trust between sensor nodes is essential one [2].

2. PROPOSED CONTRIBUTION

In this section, a description of the proposed approach and its formalization is described to be more clear.

2.1. Description

Deployed in a hostile environment, individual nodes of WSNs could be easily attacked by the adversary due to the constraints such as limited battery lifetime, memory space and computing capability. It is critical to detect malicious attacks in order to avoid being misled by the falsified information injected by the adversary through compromised nodes. In this context, the WSN attacks are categorized into internal and external attacks. The external attack is performed by some external entities aiming at deteriorating the WSNs functionality. So, we will extend the idea proposed by [5], that achieves data integrity against the data falsification. It is the first schema that attempts to add security based on watermarking to LEACH routing protocol. While, internal WSN nodes that act selfishly or maliciously are considered as internal attacks. This leads to introduce new trust models into Watermarking-LEACH schema to infer the total trust and security also with the energy-efficiency.

Watermarking-LEACH schema can be used in prevention of external attacks in WSNs but they cannot block internal attacks. So, the proposed approach combines the trust model with the Watermarking-LEACH to analyze node behaviour and identify the selfishness attack and falsification at the same time treat the energy efficiency. In order to improve the robustness, this paper proposes an improvement in Watermarking-LEACH schema called Trust-Watermarking-LEACH (T-W-LEACH). The trust management component deployed on nodes to calculate the trust value, elect the reliable cluster-head and record the remaining energy for preventing internal attacks. The watermarking component deployed on nodes to construct and extract watermark for ensuring the integrity of the data against the data falsification.

2.2. Model and Formalization

As shown in Figure 1, the Trust-Watermarking-LEACH contribution contains two essential components:

The trust management component is deployed on nodes to calculate the trust value, elects the reliable cluster-head (CH) and records the remaining energy. Therefore, trust management is a solution for a compromised network and preventing internal attacks.

The watermarking component is deployed on nodes to construct and extract watermark to ensure the integrity of the data against the data falsification and ensures the energy efficiency at the same time.

2.2.1. Trust Management Component

The trust management component contains two essential phases, trust module and routing module. The Routing part is same as the Watermarking-LEACH [5], but the cluster head selection is dependent on trust value. The new trust values are calculated and shared among cluster-heads. In this trust model into Watermarking-LEACH schema, every node has 4 components running on it: Energy-Component (E-C), Trust-Component (T-C), Watermark-Component

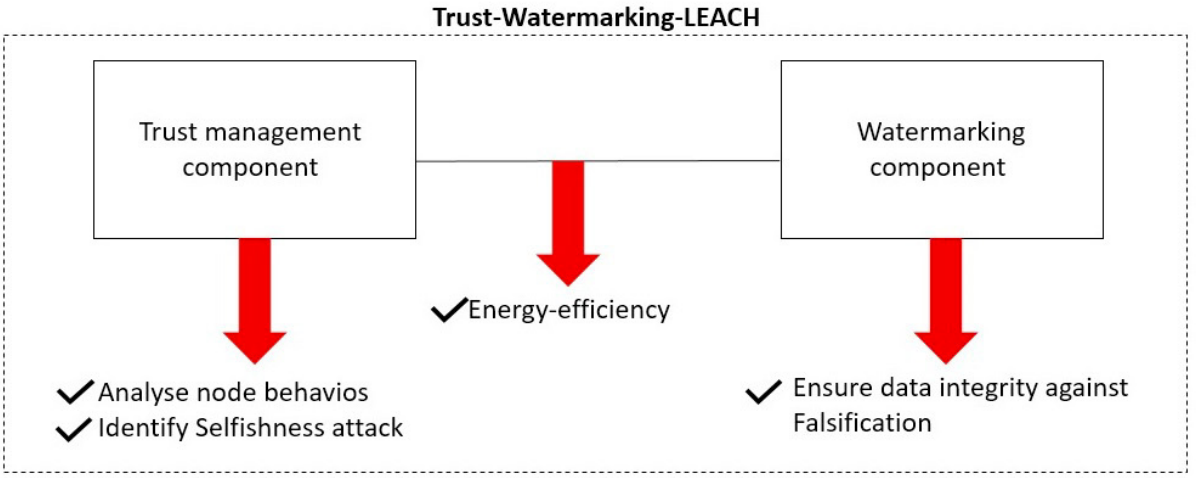

Fig. 1. Trust-Watermarking-LEACH Representation.

(W-C) and Distance-Component (D-C). A sensor node is denoted by: Node (E-C, T-C, W-C, D-C). Components are detailed in Figure 2.

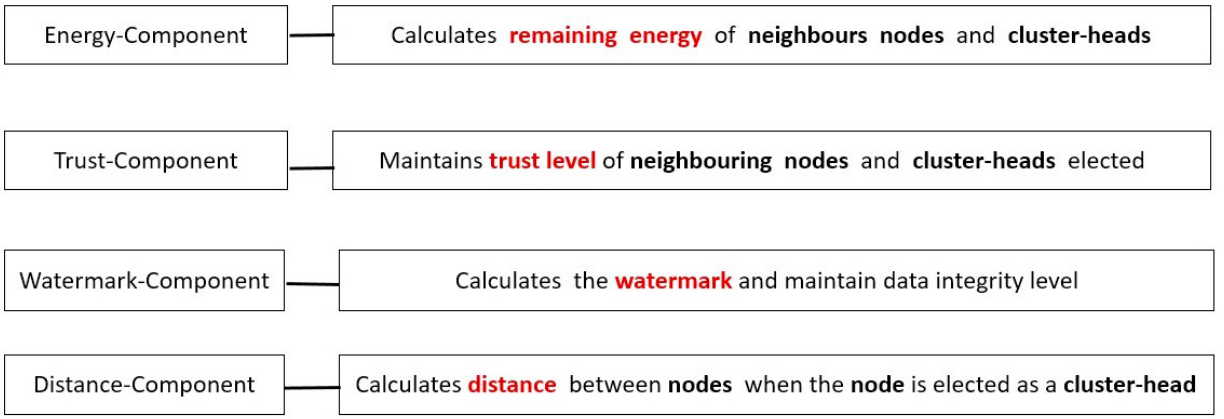

Fig. 2. Components Running on Node of Trust Model.

2.2.2. Phase 1: Trust module

For calculating trust, the T-C calculates direct and indirect trust. The final trust is calculated by aggregating direct and indirect trust values.

After that, the T-C stores all final trust values of nodes.

Direct trust

In this trust phase, the calculation of Direct-trust is based on interactions of nodes. The energy and distance are considered as a trust metric given by the following equation:

$$Direct - trust_{(A-B)} = \frac{Er}{d_(nodeA, nodeB)} \tag{2}$$

Attributes of the equation eq1 are explained in 1. By the equation (1), we can conclude that more the Er, more will direct trust calculated. Less d(nodeA, nodeB), more will the trust level [2].

Table 1. Attribute of the equation eq1

Attribute	Description
$Direct - trust_{(A-B)}$	direct trust value calculated by A for B
Er	remaing energy of node B
$d_{(nodeA,nodeB)}$	difference distance of nodes A and B

Indirect trust

The calculation of Indirect-trust is based on recommendations of nodes. Indirect-trust is the sum of trust values calculated by other nodes and given by eq2 [2]:

$$Indirect - trust_{(A-B)} = \sum Direct - trust_{(}A - C) \times Direct - trust_{(}C - B) \tag{3}$$

Table 2. Attribute of the equation eq2

Attribute	Description
Indirect-$trust_{(A-B)}$	Indirect trust value calculated by A for B Considering recommendation from C ; C A
Direct-$trust_{(}A - C)$	direct trust value calculated by A for C
Direct-$trust_{(}C - B)$	direct trust value calculated by C for B

Attributes of the equation eq2 are explained in 2.

Final trust

For calculating final trust both of direct and indirect trust will be aggregated as given by eq3 [2]:

$$Trust_{(A-B)} = wDirect - trust_{(A-B)} + (1 - w)Indirect - trust_{(A-B)} \tag{4}$$

Table 3. Attribute of the equation eq3

Attribute	Description
$Trust_{(A-B)}$	Final trust of node A on node B
w	Weight associated with direct and indirect trusts

When w is higher means that the decision of node depend on its own judgment. When w is lower means that the decision of node depends on recommendations provided by other nodes.

2.2.3. Phase 1: Routing module

Setup phase

This phase is similar to the watermarking-LEACH protocol but we make a change on the selection of C-H. In the watermarking-LEACH protocol, nodes are distributed randomly on a specific area and thus possible that the nodes are far from C-H, leading to an acceleration in the death of nodes. It's possible that there will be two nodes or more neighbouring leading to send information identical to C-H and this increases energy consumption and reduces the network lifetime. So, the nodes with less energy should not get selected as C-H. The number of nodes elected as C-H will be less and thus increasing network lifetime. Nodes will be selected as C-H based on threshold value given in eq4.

$$T(n) = \frac{p}{1 - p \times rmod\frac{1}{p}} \sqrt{\frac{E_r}{E_i}}; n \in G \tag{5}$$

Table 4. Attribute of the equation eq4

Attribute	Description
p	desired percentage of cluster heads
r	current round
Er	remaining energy of node
Ei	initial energy of node
G	set of nodes not elected as cluster-heads in the last 1/p rounds

After this phase, nodes have list of all eligible C-H members.

Trusted cluster head

After selection of cluster-head (CH), now the elected CH will find all its CH neighbours and all information regarding CH neighbours will be collected from 4 component described above. CH will maintain information of neighbours CH in form of a table. Each node will maintain an entry corresponding to every attribute as below 7.

Table 5. Neighbours CH Table

Attribute	Description
ID	ID of neighbour node
$\text{Trust}_{(A-B)}$	Final trust of node
Er	remaining energy of node
EC	How many times node is elected as cluster head
Nn	if neighbour is nearest or no

In this step, cluster-head (C-H) search the nearest neighbor node by comparing neighbor values distance with D given by Equation eq5 [2].

Distance between nodes is calculated with signal strength. If distance $\leq D$; *then* $N_n = 1$. *else* $N_n = 0$.

$$D = i\sqrt{\frac{1}{\Pi S}} \times L \tag{6}$$

Table 6. Attribute of the equation eq5

Attribute	Description
L	length of the area where nodes are deployed
i	adjusting factor
S	number of cluster-heads

If number of $N_n \geq 0$ then Cluster head calculates trust weight W_trust associated with every nearest Cluster head neighbour.

W_trust is calculated by the equation below:

$$W_{trust} = \alpha \times \frac{E_r}{E_i} + \beta \times \frac{Trust_{(node)}}{\sum Trust_{(node)}} + \gamma \times \frac{d_{(CH,BS)}}{ad_{(C-H,BS)}} + EC \tag{7}$$

Cluster-head with weighty W_trust value is selected as new cluster-head and broadcast this information to other nodes. Also, the minimum distance of node from BS is considered. $d_{(CH,BS)}$ is compared with others $d_{(CH,BS)nodes}$: If the difference between CH and BS is greater than predefined value, node will not be selected as cluster-head.

Table 7. Attribute of the equation eq6

Attribute	Description
α, β, γ	weight factors
EC	How many times node is elected as cluster head
$\sum Trust_{(node)}$	aggregation of trust of all nearest neighbour
$d_{(CH, BS)}$	distance between cluster-head and base station
$ad_{(CH, BS)}$	acceptable distance between cluster-head and base station

When the trust value of the sensor nodes was less than the threshold, the cluster heads were disconnected to help on reducing the energy consumption.

Cluster selection

In the watermarking-LEACH protocol [5], non-cluster head nodes join cluster based on signal strength received from CH but in the proposed trust-watermarking-LEACH, nodes will select their cluster-head based on trust values of cluster nodes. Cluster-head will be selected with help of equation eq7:

$$W_{CH} = x \times \frac{Trust_{(node)}}{\sum Trust_{(node)}} + y \times \frac{d_{(node,CH)}}{ad_{(node,CH)}} \quad (8)$$

Table 8. Attribute of the equation eq7

Attribute	Description
x, y	weight factors
$d_{(node, CH)}$	distance between node and cluster-head
$ad_{(node, CH)}$	acceptable distance between node and cluster-head

Schedule module

After receiving messages from nodes, C-H creates a TDMA schedule and assigns time slots to non-cluster nodes to send data as well as to calculate trust.

After that, CH generates the watermarking information (mark1) then aggregates and transmits it to the base station (BS).

Steady state phase

In steady state phase, nodes will transmit sensed data to CH along with calculating trust. In this step, the base station extracts the watermarking information expressed as (mark2) and recalculates the watermark: if mark1 is equal to mark2, the data integrity has not been falsified during the transmission.

2.3. Watermarking Component

The Watermarking Component contains two essential phases: the construction phase and the extraction phase. In the construction phase, each local cluster-head sets a watermark for each sensor data after receiving sensed data with calculating trust. In the extraction phase, at the receiver, the BS applies a function to verify the data integrity. For more details about watermarking-LEACH Protocol, see [5].

3. EXPERIMENTATION AND DISCUSSION

In this section, the proposed T-W-LEACH scheme is compared and validated. Firstly, we designed and implemented a simulation of WSN by using MATLAB tool. Secondly, Security and Energy Evaluation is realized. Thirdly,

a comparative analysis of the proposed technique is performed with TBE-LEACH a Trust based energy efficient routing in LEACH for wireless sensor network [8].

3.1. Experimentation Results

In this simulated WSN, we consider 100 nodes. All nodes are randomly distributed. The parameters of the simulation experiments are described in Table 9. It permits us to see the metrics and behaviour of a sensor and evaluates the performance of the proposed schema.

Table 9. Parameters Simulation Settings

Parameters	Values
Simulation Area	100X100
Number of sensor nodes	100
Initial Energy of Node	0.5 J/node
Routing protocol	our proposed watermarking-LEACH

We have simulated TBE-LEACH a Trust based energy efficient routing in LEACH for wireless sensor network [8] and the proposed T-W-LEACH a Trust-Watermarking-LEACH algorithm in MATLAB to make comparative analysis.

TBE-LEACH protocol			**Our proposed T-W-LEACH protocol**		
No of round	First dead node	Dead node in 500 round	No of round	First dead node	Dead node in 500 round
1	290	30	1	312	22
2	331	21	2	350	17
3	314	28	3	332	19
4	356	31	4	370	15
⋮	⋮	⋮	⋮	⋮	⋮
560	298	35	560	391	9
561	380	38	561	366	27
562	304	26	562	400	6
⋮	⋮	⋮	⋮	⋮	⋮
900	402	45	900	434	23
⋮	⋮	⋮	⋮	⋮	⋮
1000	386	35	1000	406	18

Fig. 3. Comparison of Death Nodes in TBE-LEACH and T-W-LEACH.

3.2. Security Evaluation

We make evaluation in both TBE-LEACH and T-W-LEACH protocol through 1000 rounds to compare their performance.

3.2.1. Evaluation against falsification

The Impact of falsification in this work is determined by evaluating the FNR. Firstly, we show the result without falsification and record FNR values both to TBE-LEACH and T-W-LEACH. Secondly, we consider the network attacked by a malicious sensor node. We execute a slight script for injection a false data to introduce falsification in data wireless sensor networks. Finally, we evaluate the difference between the FNR values with the result without the falsification. The FNR values are low on T-W-LEACH compared to TBE-LEACH. So, we can conclude that the watermarking is the best technique to overcome data integrity and detects false data injection using hash function.

3.2.2. Evaluation of Trust Value

In this paper work, the trust evaluation component was added to the watermarking-leach protocol.

The simulation results in both TBE-LEACH and T-W-LEACH protocol indicate that the trust value can be reduced if suspected behaviour was present. In this case, T-W-LEACH with the trust model has fewer dead nodes compared to the previous scheme watermarking-LEACH. Also compared to TBE-LEACH, the proposed T-W-LEACH model had fewer dead nodes as shown in Figure 3 because when the trust value of nodes was less than the threshold, the C-H was disconnected to help on reducing the energy consumption.

3.3. Energy Evaluation

After the implementation of TBE-LEACH and T-W-LEACH for 1000 experiments as maximum of rounds. Figure 3 summarizes comparative results measures and Compartive of death nodes for both protocols. TBE-LEACH and the proposed T-W-LEACH have a small difference in reducing energy consumption. The simulation results show that the dead nodes depend on the selected cluster-head because it depends on the threshold and nearest nodes (Distance to the cluster-head) as explained above. So, we can conclude that both protocol are efficient in reducing energy consumption. As we can see in Figure 3, in the proposed approach fewer dead nodes are compared to TBE-LEACH. So, we can conclude that the trust model into leach-watermarking model help on reducing the energy consumption, when the trust value is less than the threshold. TBE-LEACH a Trust based energy efficient routing in LEACH for wireless sensor network and T-W-LEACH a Trust-Watermarking-LEACH achieving energy-efficient. Morever, had a small differences in reducing energy consumption. Both protocols, TBE-LEACH and T-W-LEACH preventing internal attack and ensuring a secure reliability. TBE-LEACH does not work against falsifications. The proposed Trust-Watermarking-LEACH:

- Preventing internal attacks
- Ensuring the data integrity against the data falsification
- Ensuring the energy efficiency

The simulation results demonstrate the effectiveness of this proposed scheme.

4. Conclusion

In this paper, we proposed a secure and energy-efficient trust model into the Watermarking-LEACH approach. The main contribution of this work is a combination of a trust model into leach-watermarking schema to prevent at the same time internal and external attacks. This trust-Watermarking-LEACH (T-W-LEACH) achieving data integrity against falsification and analyzing node behaviour to identify the selfishness attack at the same time treat the energy efficiency. The implementation and simulation of T-W-LEACH is done with the MATLAB tool simulator and the evaluation of security and energy is made to perform a comparative with TBE-LEACH a Trust based energy efficient routing in LEACH for wireless sensor network. This paper demonstrated high reliability and showed calculation of trust for nodes, trusted cluster head selection, secure routing and watermarking construction and extraction. Evenly, this trust-watermarking-LEACH schema ensures the security against selfishness attack and falsification. The energy efficiency is also considered.

References

[1] X. Huang, D. Sharma, M. Ahmed, Security Computing for the Resiliency of Protecting from Internal Attacks in Distributed Wireless Sensor Networks. 12th International Conference on Algorithms and Architectures for Parallel Processing. Fukuoka, Japan, 2012.

[2] Amol R. Dhakne, Prashant N. Chatur, TCNPR: Trust Calculation based on Nodes Properties and Recommendations for Intrusion Detection in Wireless Sensor Network, IJCSNS International Journal of Computer Science and Network Security, Vol. 16, No. 12, 2016.

[3] Momani M. Bayesian, Methods for Modelling and Management of Trust in Wireless Sensor Networks, Ph.D. Thesis, University of Technology, Sydney, 2008.

[4] Lopez. J, Roman. R, Agudo. I, Fernandez-Gago. C, Trust Management Systems for Wireless Sensor Networks: Best Practices, Computer Communications, 2010.

[5] Nejla. Rouissi, Hamza. Gharsellaoui, Improved Hybrid LEACH Based Approach for Preserving Secured Integrity in Wireless Sensor Networks, International Conference on Knowledge Based and Intelligent Information and Engineering Systems, KES2017, Marseille France, 2017.

[6] Boubiche. Djallel Eddine, Secure data aggregation watermarking-based scheme in homogeneous WSNs (SDAW). Telecommunication Systems, 2015.

[7] V. Dhiman, P. Khandnor, Watermarking schemes for secure data aggregation in wireless sensor networks, A review paper In Proceedings of 2016 International Conference on Electrical, Electronics and Optimization Techniques (ICEEOT), 2016.

[8] Arzoo. Miglani, Tarunpreet. Bhatia, Shivani. Goel, TRUST based energy efficient routing in LEACH for wireless sensor network, Proceedings of 2015 Global Conference on Communication Technologies(GCCT 2015), 2015.

[9] Gauri. Kalnoor, Jayashree. Agarkhed, Intrusion Threats and Security Solutions in Wireless Sensor Networks. International Robotics Automation Journal, Vol. 4, No. 1, 2018.

[10] Muhammad R. Ahmed, Xu. Huang, Dharmendra. Sharma, A Taxonomy of Internal Attacks in Wireless Sensor Network, International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering, Vol. 6, No. 2, 2012.

[11] Harpreet. Kaur, Attacks in Wireless Sensor Networks(WSN), An International Journal of Engineering Sciences, 2010.

[12] Guangjie. Han, Jinfang. Jiang, Lei. Shu, Jianwei. Niu, Han-Chieh. Chao, Management and applications of trust in Wireless Sensor Networks: A survey, Journal of Computer and System Sciences, Vol. 80, No. 3, 2014.

[13] Swathi B.H, Gururaj H.L, A Critical Analysis on Network Layer Attacks in Wireless Sensor Network, International Research Journal of Engineering and Technology (IRJET), Vol. 05, No. 02, 2018.

[14] Bharath. Bhushan, Gadhar .sahoo, Recent advances in attacks, Technical challenges, vulnerabilities and their countermeasures in Wireless sensor networks, 2017.

[15] Shivani. Garg, Mukul. Varshney, Aparajita. Nailwal, Insider Threats in Wireless Sensor Networks and Their Countermeasures, International Journal of Computer Science and Mobile Computing(IJCSMC), Vol. 5, 2016.

[16] F. Fanian, M-K. Rafsanjani, V-K. Bardsiri, A Survey of Advanced LEACH-based Protocols, International Journal of Energy, Information and Communications, 2016.

[17] M. Bani Yassein, A. Al-zou'bi, Y. Khamayseh, W. Mardini, Improvement on LEACH Protocol of Wireless Sensor Network(VLEACH), 2009.

[18] Nazia. Farooq, M. Abdul, A Survey on Energy Efficient Clustering Protocols in Wireless Sensor Networks, International Journal of Computer Applications, 2018.

[19] Heydar. Ghasemzadeh, Mehdi. Rezaeian, Fatemeh. Dehghan Touranposhti, Mohammad Mohsen. Ghasemian, An improvement on LEACH protocol using Bayesian networks for energy consumption reduction in wireless sensor networks(BN-LEACH), 7'th International Symposium on Telecommunications (IST'2014), 2015.

[20] Rekha. Rani, Rajan. Manro, Improved Watermarking Leach Protocol using node level Integrity and Confidentiality in WSN, INTERNATIONAL JOURNAL OF COMPUTER SCIENCES AND ENGINEERING, November 2018.

[21] Reshma I. Tandel, Leach Protocol in Wireless Sensor Network: A Survey, International Journal of Computer Science and Information Technologies(IJCSIT), Vol. 7, 2016.