Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Secure Routing Protocol for Low-Energy Medium and Large Wireless Sensor Networks

Dr. Sasivardhan Thota[1], Dr.B. Rebecca[2], Dr. JaishriWankhede[3], Dr. U. Mohan Srinivas[4], K Little Flower[5], Shaik Jasmine[6], Dr.G.Charles Babu[7], Dr. Neeraj Sharma[8]

[1]Assistant Professor, Department of Artificial Intelligence and Data Science, School of Technology, GITAM(Deemed to be University), India
[2]Associate Professor, Computer Science and Engineering, MarriLaxman Reddy Institute of Technology and Management, India
[3]Professor, Department of CSE, CMR Institute of Technology, India
[4]Professor, Department of CSE-AIML, Malla Reddy Engineering College(A), India
[5]Associate Professor, Department of CSE, St. Peters Engineering College, India
[6]Assistant Professor, Department of CSE, GokarajuRangaraju Institute of Engineering and Technology, India
[7]Professor, Department of CSE, GokarajuRangaraju Institute of Engineering and Technology, India
[8]Professor, Information Technology, Vasant Dada PatilPratishthan College of Engineering and Visual Arts, (VPPCOE&VA), GokarajuRangaraju Institute of Engineering and Technology, India
Email: sthota6@gitam.edu

Wireless Sensor Networks are networks consisting of a large number of low-power sensor nodes and can vary. This article proposes two secure routing protocols against various attacks with the new key management method. These protocols are proposed for two different environments. The first protocol is designed for small/medium-sized networks, while the second protocol is designed for large-scale environments. Both protocols consist of three phases: the network formation phase, the security, switching phase, and the data transfer phase. The protocols, which have the same first and third phases, differ only in the second phase. In these two phases, the network will be created using the proposed new virtual layer and data transfer will be done efficiently. With the development of the 'multi-symmetric key' technique in the first protocol, reducing the load of the system and making energy consumption efficient is successful against routing attacks such as Wormhole, Sybil, Hello flood, and DoS. In the second protocol, it is used only by cluster heads/active nodes and switch servers, making energy consumption efficient and preventing DoS, traffic analysis and physical attacks. When the developed protocols are compared to LEAP, LEAP+, BROSK, LISP, SABR, and PASSWORD, it is seen that they are successful in performance.

Keywords: Wireless networks, Secure Routing Protocol, Energy efficiency, Key management.

1. Introduction

Wireless Sensor Networks (WSNs), which are from the family of wireless ad-hoc networks, are networks that consist of a large number of sensor nodes and can vary. WSNs are of many different types of thermal, magnetic and visual structures that can follow situational changes such as humidity, temperature, pressure sensor. The information detected by these nodes is collected at the base station and transmitted from there to the server. The server side is a centralized data collection and analysis system. Operators who are on the server side can constantly monitor the status of network components. WSNs can self-configure in a short period of time with minimal configuration and can be easily spread over a wide area [1]. These networks, whose current standard is IEEE 802.15.4, are networks that are required to communicate with minimum system resources because they are powered by batteries. Nodes in these networks typically reach the end of their useful life when their batteries run out. Apart from the battery problem, the memory of the sensor nodes is also limited [2]. The limited processing power, memory, bandwidth, and supply resources of the sensor nodes can make their WSNs vulnerable to a variety of attacks.

Due to the limited resources of WSNs the security mechanisms(secure routing rationale, secure location justification, continuous topology change feature, secure key generation, secure data clustering, etc.), of non-ad-hoc networks cannot be used in these networks [3]. In areas such as military and medical tracking systems, the security of these networks is of great importance. WSN security is examined under four headings as Key Management, Intrusion Detection, Secure Routing and Secure Positioning [4]. Due to the dynamic nature of the WSN, the easy reconciliation of nodes, and its self-organization, key management is very complex.Due to their limited communication and computational capacity, WSNs are vulnerable to various attacks. In many cases, attackers can find a way to infiltrate the network, no matter how these networks are designed. Intrusion detection systems can detect these attacks based on illegal events. WSN uses multi-hop routing and wireless communication to transmit data because the middle node needs to reach the data message content. Therefore, these networks can be exposed to many types of routing attacks. Since traditional end-to-end security mechanisms cannot provide communication in wireless network systems, there are many approaches that address routing security. In WSN, location information is very important in some applications, such as reaching coordinates in hostile environments. In such applications, location information or distance information between neighbouring nodes is needed in many routing protocols or other security mechanisms. WSN attacks are divided into two as internal and external attacks [5]. In internal attacks; The attacker attacks by obtaining the sensor nodes and the secret key. In external attacks, the attacker attacks in a way that disrupts the function of the target sensor network with its own sensor nodes without having the secret key information. These attacks can be node capture attacks, channel attacks, denial-of-service attacks, redirect attacks, traffic analysis attacks, and Sybil attacks.

The most important and dangerous of these attacks is denial of service Denial of Service (DoS)

attacks. DoS attacks are defined as the obstruction of the task expected from the WSN or the reduction of its performance to a great extent. DoS attacks can easily occur due to the structure of WSN on the developed system.Typically, in a DoS attack, an attacker hijacks a node and sends unnecessary packets to consume resources on the network and prevent other sensor nodes from taking advantage of the network's resources or services. In addition, DoS attacks can be carried out at other layers of the network. At the physical layer, DoS attacks impede communication by creating noise and compression. DoS attacks occur in the form of collisions, fatigue and unequal behaviour at the link layer. At the network and routing layer, there are DoS attacks in the form of packet drop and misdirection, black and wormholes. In the transport layer, there are DoS attacks in the form of desynchronization. Against these attacks, it is possible to implement secure routing protocols by using resource usage charges, strong authentication, traffic identification and switching management methods.

Although there are many studies on the efficiency and usability of these networks, there are not enough studies in the field of security of these networks. In this article, the new key management methods and secure routing protocols introduced will accomplish the objectives of data privacy, authentication, data integrity, availability, data freshness, time synchronization, and secure positioning.

In the second section of this article, studies in the literature are examined. In the third and fourth sections, the development of the proposed protocols andperformance analyses are explained. In the last section, there are conclusions and recommendations.

2. Literature Survey

The most important techniques that can provide security in WSNs are key management and encryption methods [6]. However, these methods not only provide security, but also increase energy and memory expenditure. Therefore, the presented methods should perform both parameters in a balanced way. Encryption methods are divided into two classes as symmetric and asymmetric. Asymmetric encryption methods are not considered appropriate for use in these networks because they are not efficient in memory and energy consumption [7]. Therefore, studies in the literature for WSNs are generally carried out on symmetrical methods. These symmetrical methods are divided into two categories.

2.1 Central Structure:

It uses a central structure to perform the key distribution process. The most well-known studies in this category are the SPINS [8], SNEP [9] and Karlof [10] protocols. The SPINS protocol uses the SNEP to achieve its privacy purpose, as well as the μTESLA [11] method to provide authentication. However, these protocols can lead to premature collapse of the system because they use a centre-based structure. Because central architectures resemble star topology. In addition, the scalability characteristics of such methods are limited and they are open to various attacks.

2.2 Distributed Structure

The second category of symmetric switching methods are protocols that use distributed structure. In this category, protocols distribute keys in a distributed structure. This category is

divided into two classes.

2.2.1 Random Distributed Structure

In this structure, each node tries to generate random public keys to communicate with its neighbour. In order for the nodes to communicate with each other, the protocol must generate the same key on the nodes. This process has to continue until it generates the same key. Therefore, it causes excessive energy consumption of the network and is not considered suitable in large-scale systems.On the other hand, protocols in this class do not have a stable state [12]. In this class of methods, "key pre-distribution" and "probability switch" techniques are used. The random pairwise [13] protocol distributes random keys to all nodes by creating a single key pool. Some nodes selected as coordinators will have all the key information, so the security of the system will be at great risk if these nodes are taken over by the enemy. To address this issue, the q-Composite [14] protocol has been proposed. This protocol has elevated the authentication process in key sharing between nodes from one-sided to two-sided. There are one-sided and two-sided authentication types between nodes. In the unilateral authentication technique, it will be sufficient for the receiving node to verify its identity to the sending node. However, in two-way methods, both nodes that want to communicate must verify their identities with each other.The q-Composite protocol also uses a key renewal mechanism at certain periods. However, since the key information of all nodes is kept on a few selected nodes, these selected nodes will still put the system at risk if they are compromised. Therefore, this protocol will only make the enemy's job a little harder. Another method in this class is the Polynomial-based [13] protocol. In this protocol, it is aimed to increase the security of the system by using a polynomial key pool.

However, in this protocol, the memory usage of the system will be increased and it will be more difficult to find malicious nodes. To address this issue, the Grid-based [15] protocol has been proposed. This protocol used the hamming distance and Payton functional. However, the problem of excessive energy consumption of this protocol continues. All these methods are accepted in networks with only a small number of nodes and in environments where energy is not important. Therefore, random key distribution method and centralized protocols can be used in small-scale systems that do not have energy problems. Environments without energy problems are environments where the batteries of the nodes can be easily charged. In this article, the recommended protocol for non-energy environments is presented to address the main problems in this category.

2.2.2 Deterministic Distributed Structure

Protocols using this structure provide the purposes and security of the system more efficiently than the two structures mentioned. In general, deterministic protocols use a key called master to ensure secure communication and authentication between nodes. In these methods, the security of the system can be realized in a balanced way without using much energy and memory. This structure is used in the two protocols of this article for environments where energy consumption is significant. It is also seen that the studies in the literature are lacking in this area. The most well-known studies in deterministic nature are the LEAP [16] and LEAP+ [17] protocols. These protocols are available for small and medium-sized systems. However, these protocols also have some problems. The first protocol of this study plans to focus on these methods and establish a referral mechanism to eliminate their deficiencies.In

the LEAP protocol, the one-sided generation of common binary keys leads to security deficiencies. For example, when node "u" wants to communicate with node "v", only node "v" needs to authenticate, and node "u" does not need to verify its own identity. Thus, this problem is the first shortcoming of LEAP. In the first protocol of this article, it is planned to resolve this problem by using the two-way authentication technique. The second shortcoming of LEAP is that the nodes that receive the data packet from the base station can transfer data to the nodes that are not in the base station coverage area, in the form of multi-hop, by requiring operations such as decryption and encryption. Therefore, this technique leads to excessive energy consumption. Also, in the LEAP protocol, all master keys are allocated only by the base station. Therefore, if the base station falls into the hands of the enemy, the security of the system will be at risk. In deterministic structures, this technique has been used in many protocols. This problem is the third shortcoming of LEAP. On the other hand, the distance between the base station and the nodes is also important in terms of energy consumption. Therefore, over long distances, it will be inevitable for nodes to use a lot of energy and memory. It will be inevitable for them to use energy and memory.

In recent studies in the literature, it is proposed to use a hierarchical structure to solve the problems of nodes located at long distances from the master key distribution and base station. Thanks to this structure, the protocols will distribute some of the tasks of the base station to the cluster head elements of each cluster. However, in this technique, there are still problems in terms of energy efficiency as the excess load is transferred to the cluster head elements. The first protocol proposed in this article will develop a new virtual layer structure instead of the hierarchy method in order to basically solve this problem and provide optimized energy consumption. This new virtual layer structure will introduce a new method in this area.

The most recognized protocol for deterministic and hierarchical-based studies for small/medium-sized systems is the BROSK[18] protocol. This protocol is a completely session and negotiation-based method. In this method, like LEAP, the master key given from the base station is used for key allocation between two nodes. Therefore, this protocol loses energy efficiency when the base station is far away from the nodes. The difference with LEAP is that it uses one master key. The LEAP protocol is more secure than BROSK, as a master key is more likely to fall into enemy hands.

In the literature, it is seen that the energy efficiency of nodes decreases when many studies designed for small/medium-sized networks are applied to large-scale networks. In the second protocol proposed in the article, it is planned to make energy consumption efficient by using the switching method only by cluster heads/active nodes and switch servers in large-scale networks. One of the important studies in the literature designed within the framework of distributed structure for large-scale systems is the LISP [19] protocol. In order to ensure energy efficiency, this protocol does not allocate new keys in each session, but assigns these keys at certain periods. This method is one of the successful methods in the literature because it uses the clustering structure. However, in this protocol, there are still problems in terms of energy efficiency as excessive load is transferred to the cluster head elements. Another shortcoming of the LISP protocol is that the cluster head elements do not change. Therefore, the attacker can threaten the entire system by hijacking these nodes.Therefore, it is envisaged to use the virtual layer structure in the second proposed protocol. Therefore, the problems of LISP and similar protocols will be solved. In the LISP protocol, nodes are required to use the same keys

until it is time to renew the keys allocated to the nodes. Therefore, it needs to keep the keys on the nodes for a longer period of time than LEAP and BROSK. Therefore, the use of memory will not be efficient either. In order to solve these problems, the second proposed protocol is that the active nodes, which have the keys in the virtual layer structure, change the mode according to their energy levels and distances from the base stations at certain periods. Active nodes will go into a dormant state, and dormant nodes will become active and take over. Therefore, efficient use of energy and memory will be ensured.

Many protocols in the literature, in general, only distribute keys to ensure security and do not focus on data transfer and routing. In this study, it is also planned to ensure secure communication and data transfer between nodes using new switching methods. Accordingly, two new secure routing protocols are proposed for different environments.

3. Secure Routing Protocol for Medium/Large Environments

In the literature, security targets are generally examined in different categories. In this article, it is categorized into two classes as primary and secondary. The primary goals are security criteria such as confidentiality, integrity, authentication, and availability. Secondary goals include factors such as data up-to-dateness, time synchronization, and secure positioning. In many applications, nodes are required to carry highly sensitive data or secret keys so that they do not leak their data packets to others. In this article, it is considered to encrypt the data with a secret keying method that only the relevant recipient can access and to create secure channels between nodes in order to keep sensitive data confidential. In addition, this data must be kept secret from passive attackers. In order for any message transmitted over the network to remain private, it is necessary to provide a data privacy feature. In general, data privacy; Traffic is the target of analysis and physical attackers. It is envisaged to prevent eavesdropping by using secure channel (TDMA and CDMA) and encryption methods in a hierarchical structure, to prevent physical attacks by embedding switching methods in tree-based topologies (pre-distribution, post-security), and to prevent traffic analysis attacks by encrypting general information such as the identity of the nodes. Authentication is required to prevent unauthorized access of hostile/malicious nodes. Because they use a shared wireless environment, WSN requires authentication mechanisms for malicious sniffer nodes or spoofed packet detection.

This article follows two different authentication methods for internal and external attacks. Against internal attacks, it is envisaged to use symmetric mechanisms to share secret keys between nodes. In external attacks, it is planned to use the attack detection method. In this management mechanism, system and user activities are monitored, system configuration and abnormal activity patterns are analysed, and system and file integrity is evaluated. Data integrity is automatically ensured by a trusted routing protocol after the data is kept confidential and verified. Event-based and query-based methods are used to ensure reliability.In order to achieve the availability target, it is possible to use a large number of nodes and energy-saving methods (sleep/wake-up, etc.). The availability feature protects network services from DoS attacks. To ensure data up-to-dateness, step count (hop) and time-to-live (TTL) parameters are added to each data package. Therefore, the repetition of the same packets in the network will be prevented and energy and memory efficiency will be ensured.

In order to achieve the goal of time synchronization, delays in the network are monitored by adding the packet delay parameter to the protocol. If there is a delay in the ACK of the packets, the protocol will notice this situation and decide to send the packet again. In addition, the source of the delay can also be analysed.

The final goal in this article is to provide safe positioning. Often, in order to realize this feature, the GPS location detection system needs to be integrated into the sensor nodes. Despite the location detection feature, attackers will be able to easily manipulate nodes in that area by reporting erroneous signals to unsecured locations. Therefore, apart from location detection, locations must also be safe. On the other hand, GPS mounted on each node will increase the cost of the system. With the new software method developed within the scope of this article, this feature is realized without the need for GPS.

This article proposes two protocols as a solution for two different environments. First, a protocol is designed for small/medium-sized environments. The other is that a second protocol is being developed for large-scale networks. Both protocols consist of three phases. The first phase is the formation of the network topology, the second phase is the application of switching and encryption methods, and in the last phase, data transfer is performed.

3.1 Networking Phase

The main theme of this article is the development of new secure switching routing protocols. It is aimed to prevent internal and external attacks by authenticating thanks to the correct switching and developing a secure routing protocol with new key management methods. To achieve these aims, the virtual layer structure is used in both proposed protocols. In this new virtual layer formation, it is determined which layer each node is located in by determining the number of hops between the nodes and the base station. Accordingly, the "Interest Online" message packet is broadcast to all nodes by the base station. The first value of this packet is defined as zero (HOP=0). After receiving this message, the nodes in the radio area of the base station will increase the number of the variable named HOP by 1 and send this message back to other neighbours. At this stage, the nodes that receive the new message will increase the number of the HOP variable by 1 to increase the HOP value to 2 and will transmit the message to their neighbours in the same way. So, when this message reaches all nodes, each node will have a HOP value, and it means that nodes with the same HOP values are in the same layer. The distances of the nodes to the base station are determined according to the HOP values. All these processes are summarized in figure 1. For example, a node with a HOP value of 2 means that it is located in the second layer and is two steps away from the base station.

Therefore, in this protocol, the positions of the nodes will be determined without the need for GPS and the energy consumption of the system will be efficient. To increase the energy efficiency of the network, it is enough for a few nodes per layer to remain active (figure 2). These active nodes must always be in communication with nodes in neighbouring layers, and they must be replaced by nodes that are in sleep mode between certain periods. Our protocol realizes this time interval with a parameter named T. When time T expires, a new session is opened and the active node in each layer goes into sleep mode, and the one in sleep mode goes into active mode. The number of nodes that should remain active is realized with the Connection variable (figure 3).

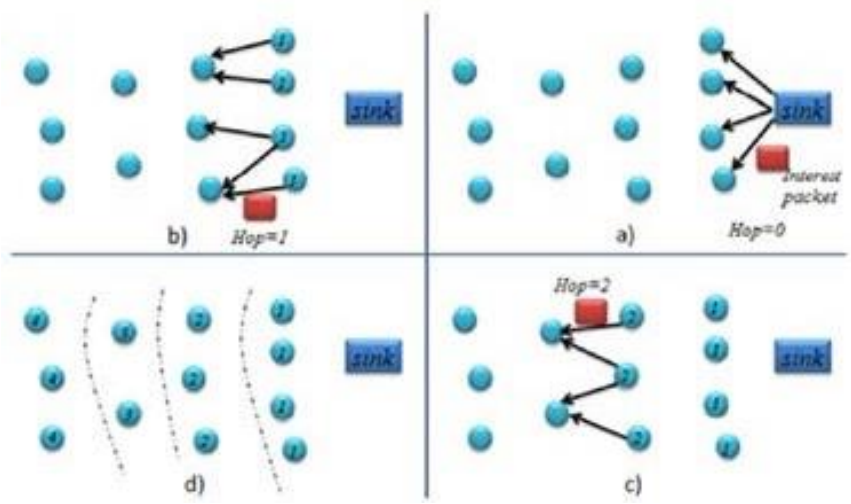

Figure 1. Formation of virtual layer.

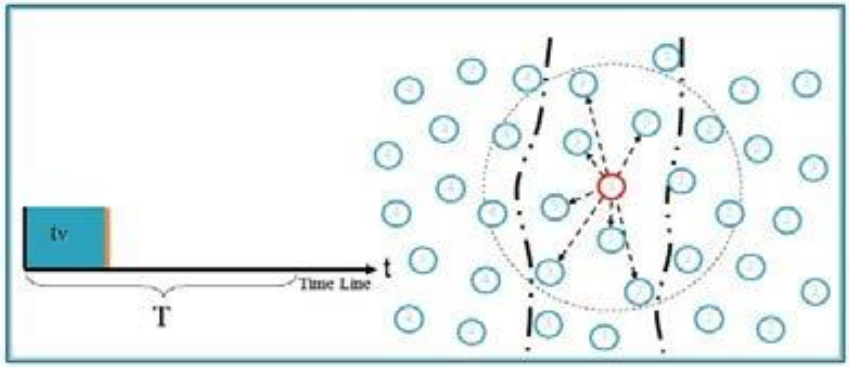

Figure2. After waiting until the active node TV, it broadcasts a HELLO message to its neighbours in its layer.

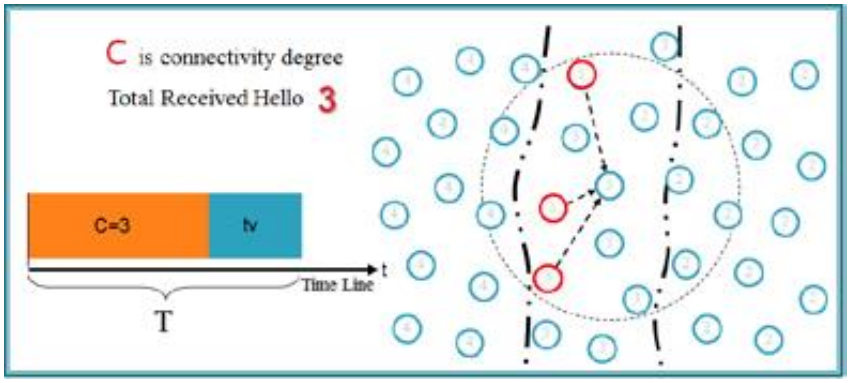

Figure 3. When there is a response from the neighbours up to the connection value, the active node goes into sleep mode.

3.2 Safety Phase

3.2.1 Protocol for Small/Medium-Sized Networks with Low-Power Energy Source

Centralized and randomly distributed structures are generally not efficient in terms of energy consumption because they use complex and heavy switching methods. Therefore, the protocols in this article ensure safety by taking into account efficient energy consumption. In the first protocol proposed, it is planned to make energy consumption efficient by reducing the load of the system by developing the 'multi-symmetric switch' technique. This technique reduces the probability of success of redirect attacks such as Wormhole, Sybil, Helloflood and facilitates system management. Alternate pathfinding and a new energy-efficient routing algorithm are other unique features of this protocol.

It is planned to eliminate the lack of inter-cluster communication and switching in LEAP and many studies in this field with the smart and multiple per cluster distribution method. Typically, in these methods, the master key is distributed from the base station to all nodes, causing them to consume a lot of energy and memory. In addition, if the base station itself is compromised by someone with bad intentions, the entire system will be compromised. In this protocol, the use of two-sided authentication technique and dynamic base stations is considered. In such environments, the distances between the base station and the nodes are important in terms of energy consumption. Therefore, over long distances, it will be inevitable that the nodes will use a lot of energy and memory. To address these problems, recent studies in the literature suggest the use of a hierarchical structure. However, as mentioned, this hierarchical structure does not achieve much success either. This problem will be addressed with the new virtual layer method (figure 1.), which will also increase energy efficiency.

In the first protocol, the new switching mechanism to increase safety and energy efficiency is presented as follows. By using the multi-symmetric key technique, attacks such as Wormhole and Sybil will be prevented.

In this technique, four types of keys will be used: "private keys" for communication between nodes and the base station, "inter-node keys" for communication between a node and its neighbours, "layer keys" for inter-layer communication of nodes, and "public keys" for broadcast shares. It is planned to carry out the following stages for the allocation of keys.

1. Private Keys: Each node will be allocated a premium key before the nodes are deployed to the environment. The information of these keys will be kept on the base station or server. The following formula is considered to be used to allocate the elite key to each sensor node.

$$K_u^m = fK_s^m(u)$$

K_u^mexpression; It means allocating a master (m) key to node "u". This master switch plays the role of a controller and is used for unique key allocation to nodes. f is a pseudo-random function. In this protocol, a unique "id" will be defined to each sensor node. The use of only one master key for the production of all keys will provide efficiency in memory consumption. This technique will be used to realize communication between the base station and the nodes.

2. Inter-Node Switches: It is planned to use this method to ensure secure communication between each node and its neighbours who are one step away. The controller will allocate the starting switch (K_1,K_2,..) to the nodes.

$$K_u = fK_1(u)$$

Next, the protocol will give nodes a certain amount of time as preparation time so that they can communicate with their neighbours. Authentication must be performed before data can be transferred between the two nodes. The period between the authentication process and the data transfer is called the "preparation time". All nodes, in the recognized preparation process, are obliged to find their neighbours.

$$\text{Node } u \leftarrow T_{min}(\text{ready})$$

During this time, nodes will wait for a response after broadcasting the "HELLO-discover" message, and when they receive a response from nodes within radio range, they will add them to their neighbour list. The authentication process will be carried out with the master key technique.

$$u \rightarrow *: \text{Nonce}_u$$

In computer science, especially in data security, the term Nonce consists of the initials of the word "number used once" and means a number used once. Each HELLO-discover message contains one Nonce number.

$$v \rightarrow u: v, \text{MAC}(K_V, \text{Nonce}_u | v)$$

The node "u" will generate a double public key between itself and its neighbour with the response from its neighbours (for example, from its neighbour named "v").

$$K_{uv} = fK_v(u)$$

When the time defined for node "u" expires, the K_1 key and the master keys allocated to all its neighbors during the discovery phase must be deleted. This process applies to each session. In this way, the security of the system will increase. At the end of each session, the allocated public binary keys will be deleted. Therefore, if any node is compromised, the security of other nodes will be protected.

3. Cross-Layer Switches: Sometimes the neighbours of the nodes can be members of another layer. In this case, there will be an urgent switching operation between neighbouring nodes that are in two different clusters. In this case, node "u" will perform the encryption process by generating a random key (K_u^C).

$$u \rightarrow v_i: (K_u^C)kuv_i$$

Next, the "v_i" node will decipher the K_u^C keys, recording them in a table. If any neighbour of node "u" is disabled for any reason (falls into enemy hands or runs out of battery), node "u" will cancel or renew the layer key and notify its other neighbors as well. In this way, the key tables of the nodes will remain up-to-date. The node "u" understands whether it and its neighbour are in the same cluster by the layer number. If it is in the same layer, the inter-node switching technique will be used, if not, the inter-layer switching technique will be used.

4. Public Key: Sometimes, depending on the need, new tasks can be transferred from the base station to all nodes of the network in the form of data packets. In such cases, it is possible to guarantee the security of the task packet sent by the public keying technique. The switching process will be done from the base station. This packet will be encrypted with the base station's own key (K_{all}^{m}) and sent to all nodes as hop-by-hop. In order to ensure energy efficiency, the transmission process of the packets sent from the base station will be undertaken by the cluster heads. The cluster head that encrypts the packet as K_{c}^{m}will continue to send this packet to other nodes that are members of the cluster where it is located. So, not all nodes in the network will have to do the constant decryption and encryption process for packet transmission. Because this process will now be done by the cluster head elements. However, the nodes that act as the head of the cluster will consume a lot of energy. The protocol will solve this problem by delegating this task to other cluster members at certain periods.

3.2.2 Protocol for Large-Scale Networks with Low-Power Energy Source

In the literature, it is seen that many studies designed for small/medium-sized networks reduce energy efficiency when applied to large-scale networks. In the second proposed protocol, it is planned to make energy consumption efficient by using the switching method only by cluster heads/active nodes and switch servers in large-scale networks. Therefore, the overhead caused by switching and encryption on the network will be reduced. This protocol will be more scalable and increase its originality by eliminating the dependency of LISP and similar studies in the literature per cluster. The protocol, which is designed for large-scale systems, will only assign new keys within certain periods. Therefore, thanks to the virtual layer structure, this method alleviates the burden of base stations or cluster heads and saves energy and reduces the possibility of security risks. In this structure, the active nodes that hold the switches change modes according to their energy levels and distances from base stations at certain periods. Therefore, efficient use of memory will also be ensured. In addition, DoS will be more resistant to traffic analysis and physical attacks. Active nodes in this structure will play a role as the head of the cluster, but unlike the hierarchy structure, the load/task on a single element will not increase.

The switching techniques used in this protocol are described below.

1. The switching method will be applied only to cluster heads/active nodes and switch servers, ensuring energy efficiency in large-scale networks and preventing DoS attacks,

2. Preventing traffic analysis attacks by using active key broadcasting that does not require ACKs to be sent,

3. It will prevent physical attacks by using the accuracy bits created without being added to the data message. It will also provide access control, control of network logins and key renewal features.

In this protocol, it is planned to use simple hashing algorithms to save energy. In addition, since the use of resources is high in accordance with this protocol, it is thought to minimize this excess by using a virtual layered structure and to keep the energy efficiency at the optimum level. An increase in energy consumption in large-scale networks is inevitable. However, it is not necessary to open a new session in inter-node communications in order to consume it in a controlled manner. Therefore, it is envisaged that the keys will be renewed periodically, not

in every session. Therefore, thanks to the timed key renewal technique, energy efficiency will be optimized. In this protocol, the same keys can be used for nodes belonging to different layers. (For example, switches allocated to nodes in layer "A" can also be used to communicate with nodes in other layers). In addition, since the task of being the cluster head (active node) can be delegated to other nodes at certain periods, the temporary key lists for the newly selected cluster heads will be updated. This protocol proposes a deterministic and stable switching method. In this direction,

a. A temporary key called T_k will be allocated to encrypt packets.

b. It will be necessary to use the master key to send the allocated T_k keys unicast to all nodes. This master key will be used as K_s. "s" can be either the base station or the cluster head element/active node.

c. The head of the cluster will undertake the task of authenticating the newly added nodes to the clusters, allocating temporary keys, notifying other nodes in the cluster, and updating the key table of the cluster.

In this protocol, the most critical part is the management of the T_ks allocated in the previous phase. Therefore, it is necessary to use a safe and reliable method of allocating new T_ks. In order to ensure this security, confidentiality and authentication processes must take place. In order to ensure reliability, it is necessary to restore the lost T_ks. In addition, the data transfer process should not be interrupted during the allocation of these new T_ks. Therefore, time synchronization [20] algorithms are needed. In this direction,

A. T_k sequence needs to be created. To perform this operation, it is planned to use a one-sided encryption method. This proposed method is similar to the S/key technique.

B. Appropriate and secure T_k distribution must be made before encryption. This task will be undertaken by the base station or the cluster head/active node, the controller packets. This package contains the following parameters.

1. t (Buffer size of the key): The size of the buffer will also be determined according to the size of the t parameter. Therefore, the level of fault tolerance will also be increased.

2. Initial T_k: It is used as the starting key.

3. T_k refresh interval: It is the process of using keys without resending against lost T_ks.

4. $T_{refresh}$: Will be used for new T_ks. The value of this parameter must be less than the refresh interval. Therefore, the latency rates in packet transmission and key renewal time will be kept at an optimal level. In addition, collisions will be avoided.

Using all these parameters is illustrated in the following formula.

$$K_s \rightarrow m: fMK_m(t|T_k|T_{refresh})$$

C. The T_k-buffering technique needs to be applied on all nodes.

D. Approval of allocated T_ks and reconnaissance and recovery of lost Tks are required. The control of the allocated T_ks depends on the sequence created. K_s, at the stage of configuring the system, will create this array.

$$T_{ki} = H(T_{ki+1}), i < n; \{T_{ki} | i = 1, .. n\}$$

The value of n must be a large number (e.g. n=100).

Apart from the task of creating arrays, K_s will also take on the task of key renewal. This will take place using the following formula.

In this protocol, the authentication process is performed secretly within the method and the size of the control packets will be greatly reduced. Therefore, energy savings will be achieved. In addition, it is planned to use three different keys for the management of these packages.

1- Initial keys: It will be used by K_s for re-key generation.

2- Update key: It will be used for periodic key distribution.

3- Request keys: If no key is assigned to the in-cluster nodes in the periodic key distribution, these types of keys will be used.

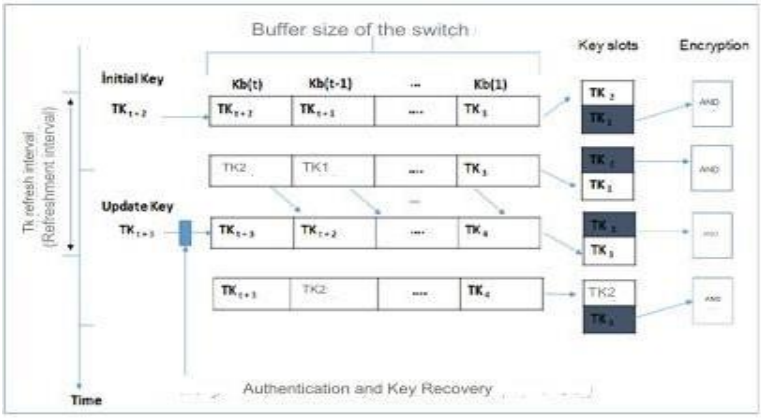

Figure 4: Management stages of allocated TCs.

3.3 Data Transfer Phase

Many protocols in the literature, in general, only distribute keys to ensure security and do not focus on data transfer and routing. The same strategy is applied in the data transfer phase for both protocols of this study. By developing a safe energy-saving algorithm, the system load on network communication will be reduced. Instead of the nodes being constantly active, by turning them into sleep mode at certain periods; It is possible to achieve this goal by preventing data redundancy and duplication by merging nodes without sending their data.

In this study, apart from the virtual layer, the use of the following techniques will ensure efficient energy consumption in data transfer.

1. By using graph and percolation theories in the virtual layer, sleep/active shifts between nodes will be intelligently controlled. In this method, the node, which is in active mode, will notify its neighbours that its task is over after a certain period of time and will be able to go into sleep mode with the response from at least the number of C neighbours. In the realization of this method, variables named T (time period) and C (connection value) will be used. In order to realize this communication model, it is planned to use graph and filtering techniques.

2. Many studies in the literature have used the technique of switching from sleep mode to active mode in software, and these projects are only It remained in the simulation stage. Sleep/active mode change is needed in hardware and electronic sciences rather than software dimension in real areas. In this article, the proposed mechanism will enable mode switching in real application areas using the TR1000 module, which is one of the best short-scope carriers. When the TR1000 module is used, the sender unit of the sleeping node will be in sleep mode and only the receiver unit will remain active. In this module, the receiver unit of the dormant node will consume 1/4 of the energy compared to the sending unit. So, thanks to this module, less energy will be consumed.

3. Alternative routes will be used for active nodes to communicate between layers. Therefore, the possibility of disconnections between layers or the occurrence of malicious nodes will be significantly reduced. In addition, both reliability and fault tolerance will be optimized.

4. In order to keep the security at a high level in data transfer, the Spanning Tree technique will be used in communication between nodes, and energy savings will be achieved at the same time.

4. Performance Analysis

Both of the protocols proposed in this article have been developed with equal parameters. These parameters with their values are shown in Table 1. These protocols were simulated with OMNET++ and compared with the top three protocols in the literature. In this experiment, MEMSIC Professional-Sensor BMT was used. For small/medium-sized environments, LEAP, LEAP+ and BROSK protocols were programmed together with the proposed protocol, and the results were obtained from OMNET++ simulation software. The comparison results are shown in figure 5. In large-scale environments, our second protocol, LISP, Password and SABR protocols. The hardware and software used are the same as those in small/medium-sized environments. The comparison results are shown in Figure 6. The input parameters required for the implementation of all protocols are used with the values in Table 1.

The first protocol was developed for small/medium environments with low power supplies and compared with studies in the literature for the analysis of operating performance. The second protocol was applied to large-scale environments and compared with studies in the literature for the analysis of study performance.

Table 1. Name and values of input parameters applied to all protocols

Parameter name	Parameter values	Parameter name	Parameter values
Initial (max) energy	0.9 J/bit	Receive buffer size	10000 bytes
Radio/ Sensor energy consumption	30 nJ/bit	Send buffer size	10000 bytes
Transmit process cost	30 nJ/bit	Deployment area size	(600 x 600) m
Receive/sense process cost	5 nJ/bit	Send/receive buffer counts	25
Data packet size	400 bytes	Sink/BS position	(600 x 300) m
Sensing Radius	7.5 m	Transmission Radius	15 m

The results of the developed protocols were compared with the protocols in other literature by

considering various output parameters. These parameters are scalability, computational overhead, communication overhead, and network lifetime. The protocol with the best performance is the one that has the highest probability of scalability and the lifetime of the network parameters, but also the protocol with the lowest values in the other three parameters. The results are not a 100% improvement, however, the protocols proposed in this article appear to achieve acceptable performance for the recommended environments. In addition, according to the results, our protocols implemented in the virtual layer structure play a major role in this improvement. Active nodes, which contain keys in the virtual layer structure, change modes according to their energy levels and distances from base stations at certain periods realizes. Active nodes will go into a dormant state, and dormant nodes will become active and take over. Therefore, efficient use of energy and memory has been ensured. In Figure 5, the first protocol proposed in the article was run with 200 sensor nodes and the results were compared with the other three protocols. In Figure 6, the same process was performed for the second proposed protocol and compared with the three most suitable protocols (LISP, Password, and SABR) recommended for large-scale environments.

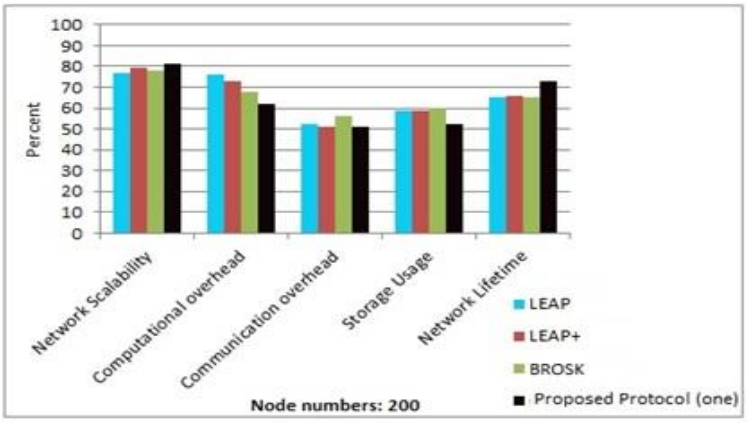

Figure-5: Comparative performance analysis of key management protocols for medium-sized environments.

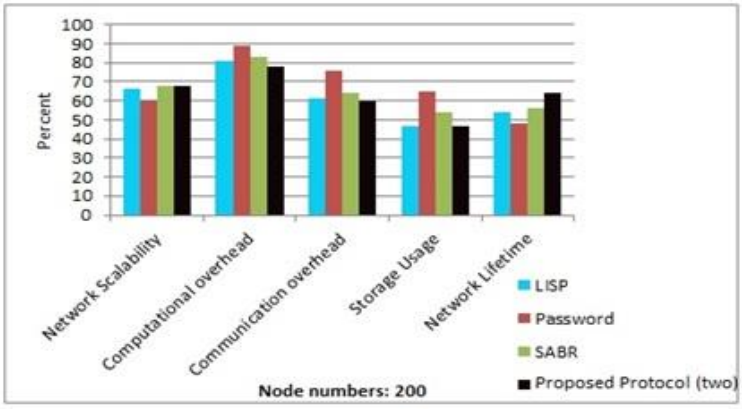

Figure-6: Comparative performance analysis of key management protocols for large-scale environments.

5. Conclusions

In this article, a new key management method and a secure routing protocol against internal and external attacks have been developed. In the proposed protocol, the first phase was carried out with two different structures (virtual layer and clustering) for network creation and different results were obtained. In the second phase, our protocol, which covers all of the purposes of switching, encryption and data privacy, authentication process, data integrity, availability, data up-to-dateness, time synchronization and secure positioning to prevent attacks, was shown with five different parameters as scalability, computational overhead, communication overhead, memory usage and network life. The results showed that the proposed protocol performed well when compared to LEAP, LEAP+, BROSK, LISP, SABR, and PASSWORD.

When the allocation of Public/Private keys is done by the base station, the possibility of a security problem still remains. Because if the base station is captured by the enemy, the entire system will be compromised. Therefore, all protocols proposed in the paper are considered to use cluster head elements, multiple base stations, mobile sensor nodes, mobile base stations, and/or Unmanned Aerial Vehicles (UAVs) for key allocation operations.

References

1. Muhammad Amir Khan, and Adnan Anwar Awan, Intelligent on Demand Clustering Routing Protocol for WirelessSensor Networks. HindawiWireless Communications and Mobile Computing, Volume 2022, Article ID 7356733, https://doi.org/10.1155/2022/7356733.
2. Rajawat, A.S.; Bedi, P.; Goyal, S.B.; Shukla, P.K.; Jamal, S.S.; Alharbi, A.R.; Aljaedi, A. Securing 5G-IoT Device Connectivity andCoverage Using Boltzmann Machine Keys Generation. Math. Probl. Eng. 2021, 2021, 2330049.
3. Rajawat, A.S.; Bedi, P.; Goyal, S.B.; Alharbi, A.R.; Aljaedi, A.; Jamal, S.S.; Shukla, P.K. Fog Big Data Analysis for IoT SensorApplication Using Fusion Deep Learning. Math. Probl. Eng. 2021, 2021, 6876688.
4. L. Sujihelen, R. Boddu, S. Murugaveni et al., "Node Replication Attack Detection in Distributed Wireless Sensor Networks," Wireless Communications and Mobile Computing, vol. 2022, Article ID 7252791, pp. 1–11, 2022.
5. M. A. Al-Shareeda and S. Manickam, "MSR-DoS: modular square root-based scheme to resist denial of service (DoS) attacks in 5G-enabled vehicular networks," IEEE Access, vol. 10, pp. 120606–120615, 2022, doi: 10.1109/ACCESS.2022.3222488.
6. KokabHavashemirezaeipour, Hamid Barati "A hierarchical key management method for wireless sensor networks",Microprocessors and Microsystems, Volume 90, April 2022, 104489, https://doi.org/10.1016/j.micpro.2022.104489.
7. X. Zhu, "Self-organized network management and computingof intelligent solutions to information security," Journal ofOrganizational and End User Computing, vol. 33, no. 6,pp. 1–16, 2021.
8. H. K. D. Sarma, A. Kar, and R. Mall, ''A hierarchical and role basedsecure routing protocol for mobile wireless sensor networks,'' WirelessPers. Commun., vol. 90, no. 3, pp. 1067–1103, Jun. 2016.
9. Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V.,Culler, D. SPINS: Security Protocols for Sensor Networks, Wireless Networks, 8(5), pp.521-534, 2002.
10. Karlof, C., Sastry, N., Wagner, D. TinySec: A Link Layer Security Architecture for Wireless

Sensor Networks, International Conference on Embedded Networked Sensor Systems (SenSys), ACM, 1, pp.162-175, 2004.

11. Du, W., Deng, J., Han, Y.S., Chen, S., Varshney, P. A Key Management Scheme for Wireless SensorNetworks Using Deployment Knowledge, IEEE InfoCom, 1, pp.13-28, 2004.
12. G. D. Devanagavi, N. Nalini, and R. C. Biradar, ''Secured routing in wireless sensor networks using fault-free and trusted nodes,'' Int. J. Commun.Syst., vol. 29, no. 1, pp. 170–193, Jan. 2016.
13. K. Selvakumar, L. Sairamesh, and A. Kannan, ''An intelligent energyaware secured algorithm for routing in wireless sensor networks,'' WirelessPers. Commun., vol. 96, no. 3, pp. 4781–4798, Oct. 2017.
14. J. Tang, A. Liu, J. Zhang, N. Xiong, Z. Zeng, and T. Wang, ''A trust-basedsecure routing scheme using the traceback approach for energy-harvestingwireless sensor networks,'' Sensors, vol. 18, no. 3, p. 751, Mar. 2018.
15. W. A. Aliady and S. A. Al-Ahmadi, ''Energy preserving secure measureagainst wormhole attack in wireless sensor networks,'' IEEE Access, vol. 7,pp. 84132–84141, 2019.
16. Ning, P., Li, R., Liu, D. Establishing Pairwise Keys in Distributed Sensor Networks, ACM Transaction Information System Security, 8(1), pp.41-77, 2005.
17. Zhu, S., Setia, S. Jajodia, S. LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks, Conference on Computer and Communications Security, 10, pp.62-72, 2003.
18. E. Alami and A. Najid,"(SET) smart energy management andthroughput maximization," Security Management in MobileCloud Computing, 2017.
19. Wang, N., Fang, S. A Hierarchical Key Management Scheme for Secure GroupCommunications in Mobile Ad Hoc Networks, Journal of System Software, 80(10), pp.1667-1677, 2007.
20. Kiani, F. A Novel Channel Allocation Method for Time Synchronization in Wireless Sensor Networks, International Journal of Numerical Modelling: Electronic Networks, Devices and Fields, 2016,pp.1-11, 2016.
21. M. Selvi, K. Thangaramya, S. Ganapathy, K. Kulothungan,H. K. Nehemiah, and A. Kannan, ''An energy aware trust based securerouting algorithm for effective communication in wireless sensornetworks,'' Wireless Pers. Commun., vol. 105, no. 4, pp. 1475–1490,Feb. 2019.