FOUNDATIONS OF COMPUTING AND DECISION SCIENCES
Vol. 41 (2016) No. 1
DE GRUYTER OPEN
DOI: 10.1515/fcds-2016-0001
ISSN 0867-6356
e-ISSN 2300-3405

SECURE ENERGY EFFICIENT ROUTING PROTOCOL FOR WIRELESS SENSOR NETWORK

Ayan Kumar Das[1], Rituparna Chaki[2], Kashi Nath Dey[3]

Abstract. The ease of deployment of economic sensor networks has always been a boon to disaster management applications. However, their vulnerability to a number of security threats makes communication a challenging task. This paper proposes a new routing technique to prevent from both external threats and internal threats like hello flooding, eavesdropping and wormhole attack. In this approach one way hash chain is used to reduce the energy drainage. Level based event driven clustering also helps to save energy. The simulation results show that the proposed scheme extends network lifetime even when the cluster based wireless sensor network is under attack.

Keywords: Wireless Sensor Network, Sensors, Hash Chain, Machine Authentication Code, Cluster, Cluster head, Security

1. Introduction

Wireless sensor networks (WSNs) are rapidly growing in their applications of controlling military activities, health care, home security and many more. WSN is composed of hundreds, even thousands of small sensor nodes, which consists of low cost, limited energy lifetime, slow embedded processors and limited memory. These resource constrained sensor nodes added with different security threats, makes WSN more challenging for the researchers. WSN introduces a combination of security threats to packet dropping, data altering and jamming. The capabilities of an adversary to eavesdrop, tamper with transmitted packets and inject packets to initiate denial-of-service (DOS) attack [7] have been enhanced due to the broadcast nature of the wireless communication medium [18]. The resource constraints limit the ability for sensor nodes to perform computation intensive public key cryptography such as RSA [1,16], though elliptic curve cryptography offers a promising course of research [11]. Thus lightweight authentication and encryption technique should be adopted. Moreover much stronger adversaries equipped with more

[1] Department of Computer Science and Engineering, BIT Mesra Off Campus Patna, das.ayan777@gmail.com, [2] A.K. Choudhury School of Information Technology, University of Calcutta, rituchaki@gmail.com,[3] Department of Computer Science and Engineering, University of Calcutta, kndey55@gmail.com

2. Related Work

The security mechanisms adopted by different hierarchical routing protocols has several pros and cons. To make energy efficient routing the network has been partitioned into clusters. In [27] the authors have used a 3D position based approach for routing in MANET and WSNs. The whole coverage area is partitioned into a number of cubic structured cells. A proactive routing table stores cell information rather than node information for reduced size. The source node checks its' routing table, and forwards the packet towards destination through the node closest to the destination. In this routing only a coarse knowledge of the dynamic network topology and the full knowledge of the partitions are required. The most of the cluster based protocols did not consider security issues in order to reduce the computational cost. The protocols with some basic security schemes have been designed to make a balance between secure communication and energy efficiency. The paper [10] presented a robust secure routing protocol based on some basic schemes such as RSA-CRT for encryption and decryption of messages, CRT [31] for safety key generation, Shamir's secret sharing principle [26] for generation of secure routes. Selection of the final route depends on the parameters such as battery power, mobility and trust value of the route. The complexity of key generation is reduced to a large extent by using RSA-CRT instead of RSA [1,16]. The comparative performance analysis showed that RSRP outperforms ZRP [29] and SEAD [15]. However the main drawback of most of the existing secure routing protocol is that more stress is given on securing the upstream flow of data packets. In many of the algorithms security demand for the downstream flow of data is ignored. Some of the existing routing protocols offer high security together with intrusion tolerance but overlooks the energy constraints of the sensor nodes to some extent. However the different types of security schemes are depicted in Figure 1.

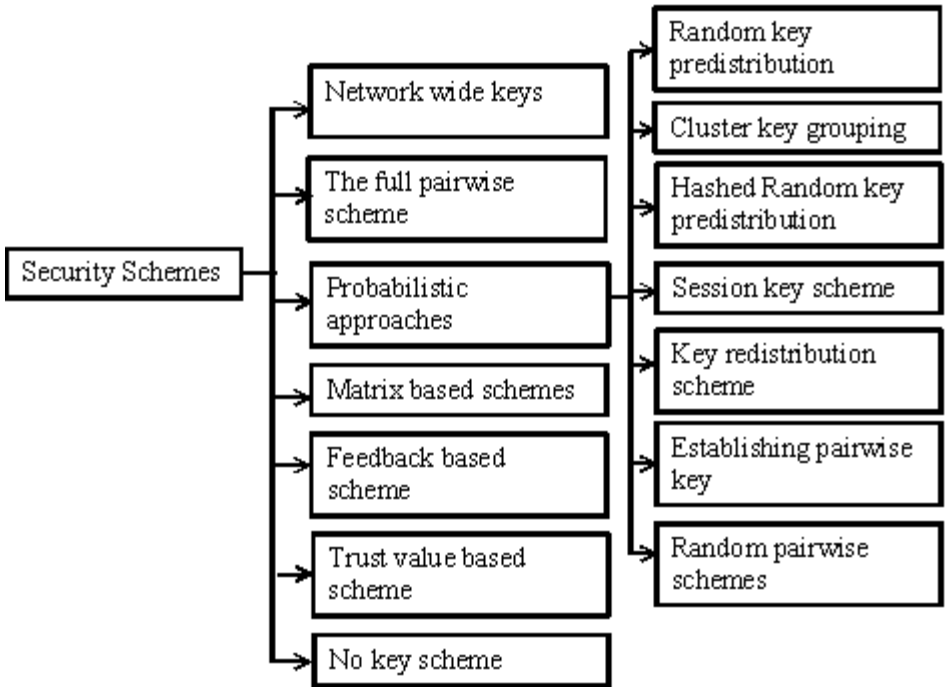

Figure 1. Types of security schemes in WSN

2.1. Network wide keys

A popular key distribution technique is to load a single master key into all sensor nodes, which results in a high level of efficiency and flexibility. It requires minimal memory for the storage. The scheme also allows the introduction of any number of sensors after the initial deployment by loading the master key in new nodes. It provides perfect key connectivity, since all nodes certainly share the same master key.

An example of such a security scheme is the BROadcast Session Key Negotiation Protocol (BROSK) [3]. In this protocol, the master key K is used in combination with random nonce NA and NB, exchanged by pairs of nodes A and B, for establishing a session key $K_{A,B}=PRF(K||N_A||N_B)$, where PRF is a Pseudo-Random Function.

In Symmetric-Key Key Establishment (SKKE) [35] scheme, nodes A and B exchange randomly generated challenges N_A and N_B. The master key K is used to compute a common shared secret as $S_{A,B}=PRF(K||ID_A||B||N_A||N_B)$. Then two keys $K_{A,B}=Hash(S_{A,B}||1)$ and $K'_{A,B}=Hash(S_{A,B}||2)$ will be created by $S_{A,B}$. A tag computed by $K'_{A,B}$ as $Tag_A=PRF(K'_{A,B}||3||S_{A,B})$, is sent by A to B, and $Tag_B=PRF(K'_{A,B}||2||S_{A,B})$, is sent by B to A. This allows the nodes to confirm the computation of the same link key $K_{A,B}$.

The Network-Wide Key approach has some security vulnerabilities. All the nodes in the network and their communications will be compromised if the adversary captures a single node and gets the common key. An attacker may easily insert malicious nodes into the network, once it has access to the master key.

2.2. The full pairwise scheme

In contrast to the previous schemes used a single master key for the communication between all sensors, in Full Pairwise scheme each of the n nodes in the network receives n-1 pairwise keys to communicate with every other node. The node-to-node authentication and perfect resilience is the cause of high security in this approach, which prevents node replication attacks. The nodes on the network identify malicious IDs and revoke the corresponding pairwise keys very easily, e.g., by using voting schemes [13,14].

The storing of many keys at every node may cause a great memory overhead. The introduction of new nodes in the network would only be possible if their keys were already loaded from the beginning, which becomes a serious restriction when the network needs to be expanded over the initial expectations. Thus the Full Pairwise Key scheme could be effectively used basically in small networks where the maximum number of nodes can be predicted with good reliability.

2.3. Probabilistic approaches

In probabilistic approaches, each node receives a group of keys, known as key chain, the size of which is normally much lower than the size of the network itself. The main objective of this approach is to reduce the memory overhead and increase the security level. The three distinct and sequential phases on such schemes are- Key pre-distribution, Shared-key discovery and Path-key establishment. The different type probabilistic approaches are discussed in the following sub-sections.

2.3.1. Random key pre-distribution scheme

The Random Key Pre-distribution scheme [20] can be considered as the basic scheme. In the Key Pre-Distribution phase, a large key pool P is initialized with |P| random keys and their respective identifiers. Then k keys are drawn at random from P to be loaded into the memory of each node to form its key chain. The exact values of |P| and k can be chosen in such a manner that each pair of nodes share at least one key with an arbitrary probability.

In Shared-key Discovery phase, each node broadcasts a list, containing the IDs of all keys in its chain. It allows a neighbor node to identify which keys they have in common.

In the Path-key Establishment phase, any pair of nodes A and B, which don't have common key, must find an intermediary node C. A suitable candidate will be any node with key chain, which contains key IDs present in both A's and B's chains. In order to create an indirect link between A and B, C can choose unassigned keys from its key chain.

This scheme is used to reduce the amount of memory for storing keys. The scalability and the resilience of the scheme are highly dependent on the sizes of the key pool and key

2.3.5. Key redistribution scheme

A modification of the random pre distribution Scheme is proposed by Law et al. [5]. In this scheme a phase called Key Redistribution replaces the original Path-key Establishment. To understand the scheme, suppose that a shared common key between nodes A and C is K_1, and that between nodes B and C is K_2. Nodes A and B don't have any common key. In the Key Redistribution phase, A checks the received IDs and asks C to send K_2 (encrypted with K_1) and to delete this key from its memory. If A gains the ownership of K_2, it now has a common key with B. In the case that C refuses to send the key, node A needs to try other keys and/or nodes until it gets a common key with B or all alternatives are exhausted. In the second case, A sends an unused key K_3 to node C selected from A's key chain. Then it return computes a reinforced key $K_{2+3}=\text{Hash}(K_2||K_3)$. This new key is encrypted with K_1 and K_2, and then both encryption results ($E_{K1}(K_{2+3})$ and $E_{K2}(K_{2+3})$), are sent back to A. Node A decrypts the $E_{K1}(K_{2+3})$ and adds K_{2+3} to its own key chain; Another result $E_{K2}(K_{2+3})$ is forwarded to node B, which takes the same procedure. At the end of this process, nodes A and B will finally have a common key K_{2+3}. Besides, after the Key Redistribution phase finishes, A has a common key with all its neighbors and, hence, some unused keys can be removed at random in order to reduce memory usage and the information that would be leaked by its capture. This approach still incurs in considerably high communication overheads.

2.3.6. Establishing pairwise keys

The Pairwise Key Establishment protocol is a solution that avoids some of the communication overhead involved in the Shared-Key Discovery phase. A good example of this type is- A Secure Aggregation Protocol for Cluster-Based Wireless Sensor Networks with no requirements for Trusted Aggregator Nodes [6], which mentions that the aggregator nodes can be the easy targets of the attackers in cluster-based wireless sensor networks. In this protocol a pair-wise key is shared between two neighbor nodes of same cluster at one hop distance which requires more storage space. Each node generates a one way key chain to authenticate its locally broadcasted messages and sends a commitment key of the key chain to each neighbor. Every node of the cluster including the cluster head broadcasts their reading to the other nodes of the cluster authenticated using the current key of the key chain. Each node including the cluster head receives the broadcasted message; the encoding key of which is authenticated checking the previously used key. After the MAC verification a local aggregation is applied on the message by each node. This process of local aggregation diminishes the need for a trusted aggregator node but consumes more energy. Finally, the cluster head computes a XOR-ed MAC over the MACs generated by the nodes of the cluster over the aggregated values and sends that to the Base station. Failure of any node or any misbehavior of a node is informed to the base station by the cluster head of that cluster.

Another protocol of this type is- A Key Management Scheme for Cluster Based Wireless Sensor Networks [23] uses public key management scheme based on ECC [2] and Diffie-Hellman [9] key exchange scheme. In this protocol each gateway node of a cluster is assigned a unique identifier. The gateway nodes are preloaded with public keys of sensor nodes, their own public keys and the public key of the base station. Each sensor node is

decision making of which nodes will take part in the routing in a secured and energy efficient manner. The feedback provided by the neighbors is authenticated with key-one way hash chains developed using μTESLA protocol. The feedback from the base station is utilized to identify the malicious nodes. Neighbors are selected dynamically and are prioritized on the basis of their last time feedback. Feedback Based Forwarding (FBF) integrates the routing layer and the MAC layer. The next packet from the sender is forwarded to a neighbor and the neighbors are reprioritized, based on the feedback value received from the neighbor nodes together with their acknowledgement sent to the sender. This scheme is well protected against sinkhole attack, selective forwarding and sybil attack. However, it is susceptible to node compromise attack.

2.6. Trust value based scheme

Energy-aware Secure Routing for Large Wireless Sensor Networks [24] selects next hop neighbor on the basis of remaining energy of the nodes and their coordinates. Direct and indirect trust information is also considered. The authors called this approach as Ambient Trust Sensor Routing (ATSR). The direct trust value is evaluated on the basis of multiple attributes like packet forwarding, network layer acknowledgements, message integrity, node authentication, confidentiality, reputation response, and reputation validation. Monitoring these attributes help in recognizing various misbehaviors of the nodes and help in avoiding certain attacks. A new node in the network calculates the indirect trust values by collecting the direct trust values calculated by the neighbor nodes. The authenticity of the calculated trust values of the selected nodes depends on their confidence factor that increases with the number of interactions of the node with their neighbors. At the time of routing nodes are selected on the basis of trust value, remaining energy and distance from the destination.

2.7. No key scheme

Security may be also implemented without using any key. One example of this type of scheme is Secure and Energy Efficient Multi-path (SEEM) [22] routing protocol. SEEM has three phases: Topology Construction, Data Transmission and Route Maintenance. Topology construction phase is for setting up the network topology; data transmission phase is the working phase, i.e., the sensor network starts its task; and in route maintenance phase, the base station updates available energy on each node, participates the communication, and reselects a new path to the source node. It has three kinds of nodes, such as sensor node, sink node and base station. The base station takes the initiative to find the multiple paths between the source node and sink node. Three types of packets are used in this protocol. They are Neighbour Discovery (ND) packet, Neighbour Collection (NC) packet and Neighbour Collection Reply (NCR) packet. This increases the control overhead of the protocol. To know the neighbour nodes of every node, the ND packet is broadcasted in the network. Then the base station broadcasts NC packet in order to collect the neighbour's information of each node gathered during the previous broadcasting. The base station will be acknowledged by the neighbour collection reply packet, sent from sensor nodes.

3. Compromised nodes of the network can launch a wormhole attack on the messages exchanged between a node and its neighbors.
4. Packet eavesdropping can be done by an intruder's node while sending the aggregated data to the base station.
5. Sybil attack can be propelled by a compromised node of the network making an illusion to the other nodes that it is present in more than one location at a time. Thus, can compel a node to forward its data to a fake node.
6. Sinkhole attack can be launched by a laptop-class attacker by advertising its high quality link and a high weight value based on which next-hop nodes are selected.

4. Proposed scheme

The proposed scheme SEER is discussed in four different modules- level formation, cluster formation with secure communication, secure data sensing and aggregation and at last sending aggregated data to the base station.

4.1. Level formation

All the nodes in the network are initialized with a level value 0. The base station checks the level value of the nodes at one hop distance to it, and if they have a level value 0, it sets the new level value of those nodes as 1. The nodes with level value 1 in turn checks the nodes at 1 hop distance from them. If the newly checked nodes have a level value 0, then the algorithm will change it to 2. This process continues till no nodes are left with level value 0.

4.2. Cluster formation with secure communication

In the cluster formation phase, the proposed scheme introduces energy efficiency by adopting an event-based cluster formation scheme, where the node that first senses the occurrence of an event initiates the cluster formation. At first all the nodes of the network calculates a competition bid value (CV) for itself as—

$$CV_i = \frac{E_{Ri} * N_{adj}}{D_{avg}} \quad (1)$$

Where for node i, E_{Ri} is the remaining energy, N_{adj} is the number of adjacent nodes and D_{avg} is the average distance of node i from all its adjacent nodes.

All the nodes that sense the event will be called as Initiator nodes. These Initiator nodes send a control message JOIN to its neighbors. Then each initiator node checks whether its CV value is highest among the neighbor Initiator nodes. If it is not highest for any Initiator node then it sends the JOIN message to its neighbor Initiator node, which has the highest CV value. This process helps the node with highest CV value to get all the sensed data from its neighbor Initiator nodes and it will be declared as cluster head. For example consider Figure2.

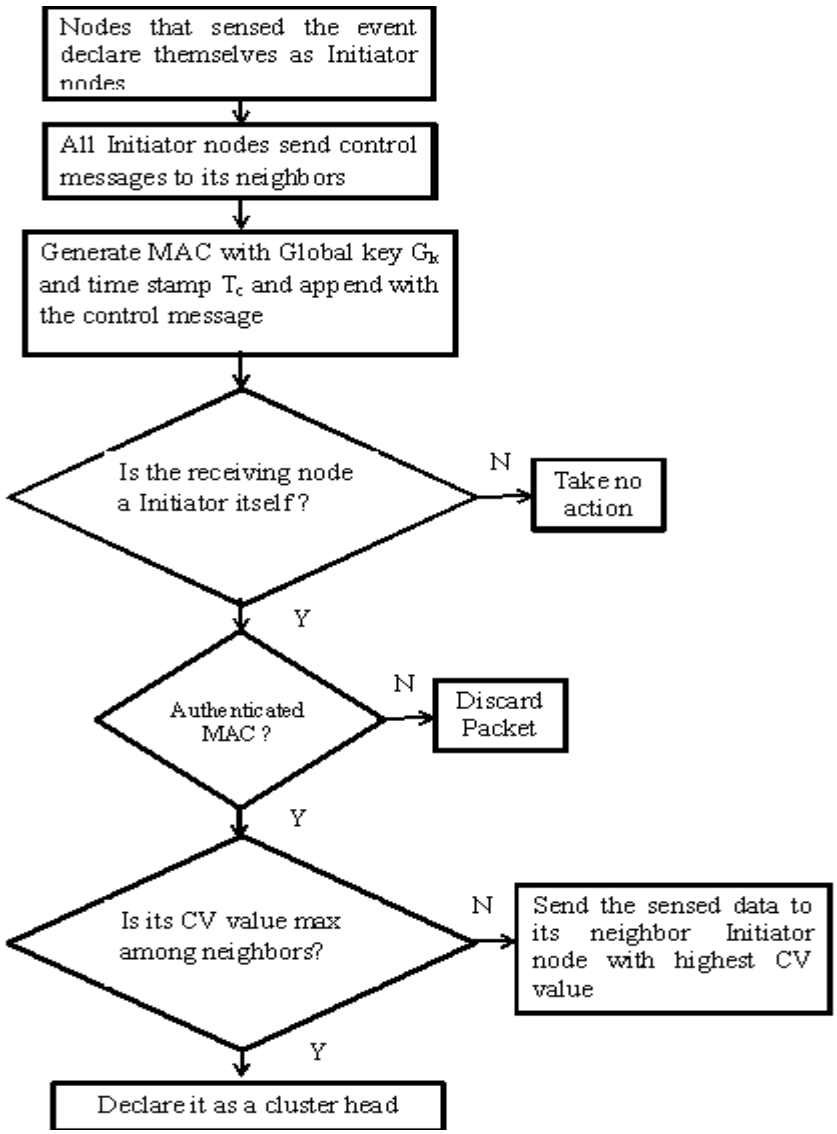

Figure 3. Flow graph for cluster formation

In SEER, the cluster will be formed only when an event occurs. The information about that event should be sent to the base station in a very short time, so that it can take corrective action as soon as possible. Thus it should not take so much time to form the cluster. The time required to form the cluster is defined in definition 1.

Definition 1:
The time required to form the cluster for N_I initiator nodes with N_{MI} number of neighbor nodes will be proportional to the MAC verification time t_m and average distance between the neighbor nodes D_{avg}. It can be defined as-

infeasible to generate within a finite time. Thus the cluster head generates a random key K_n to derive a OHC with a certain length n, such as $K_n \rightarrow K_{n-1} \rightarrow \ldots \rightarrow K_2 \rightarrow K_1 \rightarrow K_0$, where $K_{n-1} = F(K_n)$. The cluster head broadcasts the request (REQ) packet to all the member nodes of the cluster by using K_1, then K_2 and so on. No key in the key chain will be reused. The key chain will be regenerated till the last key K_n has been used. The request will be acceptable when the output of $F(F(\ldots F(K_i)))=K_0$, i.e., by i times execution of the function on K_i will be K_0, as this value is initially given to all the nodes of the network.

4.3.2. Sending sensed data to cluster head

The member nodes will send the sensed data to the cluster head, if the sent request message from the cluster head is accepted. Every member nodes append a generated MAC with its sensed data (D) to proof its authentication to the cluster head. Global key G_k is used for the generation of MAC. Thus sender (S_i) sends the sensed data (D) to cluster head (CH) with current time stamp (T_c) and a MAC generated by the global key G_k. The format of the packet is:

$$S_i \rightarrow CH : D||T_c||RE_i||MAC(G_k; D||T_c)$$

Where $D||T_c$ means the concatenation of D and T_c and $MAC(G_k; D||T_c)$ denotes that MAC is generated from $D||T_c$ with global key G_k. RE_i is the remaining energy of node i. The use of MAC guarantees the authenticity and integrity of D and use of T_c prevents the flooding attack.

4.3.3. Data aggregation and encryption

The cluster head aggregates all the collected data from its member nodes and encrypt them to prevent from altering or replace attack. The cluster head will generate any random number d to create cipher text (CT) from the original message (M) with the time stamp value T_c and the unique global key G_c. Encryption of sensed data involves the generation of key values k2 and k3 depending on T_c and G_c as follows:

a) Compute N as, $N=d*G_c$
b) Compute the first key K_1 as, $K_1= d * T_c$
c) Compute the second key K_2 as, $K_2=G_c*T_c$
d) Finally the third key K_3 is derived as: $K_3=M + G_c*K_1$
e) Now the cipher text (CT) is calculated as—

$$CT = N^{K_2 \bmod (G_c-1)} \bmod G_c + K_3 \quad (3)$$

The random number d will be sent to the receiver node (s) by appending with the packet the format of which is described in section 4.4. The CT is converted to binary form and divided into an nx8 matrix and padded according to SHA-512 formula and a required digital signature is created. This digital signature is used to validate the user identity and integrity of the data. A similar hash code is generated at the recipient site using the plain message. If the two hash codes are same, the digital signature is said to be valid and the original message is said to be unaltered.

Lemma 2: The received cipher text (CT) can be decrypted with the global key G_c and the keys K1 and K2 as in equation 8.

The cluster head is known as parent of node i. This node will calculate MAC and if it is valid, then it will be forwarded to the neighbor node with highest weight value (W_t) of its next lower level. It will replace the id of the cluster head in the packet with its own id before forwarding it. A nested MAC is generated over the received MAC from the base station using the global key (G_k), ID of the sender and the OHC. The nested MAC acts as a countermeasure against wormhole attack. The format of the request is:

$node_i \rightarrow *$: $CT||d||ID_i||OHC||T_c||TV_i||MAC(G_k; CT||OHC||T_c||TV_i||(MAC\_of\_parent))$

The above process will be repeated until the message CT reaches to the base station. Then the base station will decrypt the message and will get the original message.

5. Performance analysis

The performance of the proposed scheme SEER is analyzed and compared with three existing protocol SEEM [22], ATSR [24] and INSENS [18] as in the following sub sections.

5.1. SEER vs. SEEM [22]

In Secure and Energy-Efficient Multipath Routing protocol (SEEM) [22]base station is used as a server and the nodes are used as a client, i.e., it uses the principle similar to the Client/Server software architecture. The base station takes the responsibility of route discovery, maintenance and route selection as well. The base station periodically selects a new path based on current energy level of nodes. This protocol considers energy-efficiency and security simultaneously. The performance analysis shows that it results better in the concern of throughput, communication overhead and network lifetime. It also works well against some attacks, like Sinkhole attack.

In contrast to SEEM, SEER forms the cluster based on the occurrence of events. Though SEER is concerning about security with energy efficiency like SEEM, the cluster based approach saves more energy, as in WSN, nodes are deployed very densely and more than one node may want to send the same information about an event. SEEM is unable to face many attacks like wormhole attack, selective forwarding or hello flood attack. SEER may be used to reduce those attacks as it selects the path depending on trust value and energy of the nodes, instead of base station is choosing the path. At every move of packets SEER is checking its authenticity with the help of OHC. Simulation results show that SEER performs better than SEEM with respect to both security and energy efficiency.

5.2. SEER vs. ATSR [24]

A Scalable Geographical Routing approach for Wireless Sensor Networks (Ambient Trust Sensor Routing –ATSR) [24] adopts the geographical routing principle which offers high scalability due to its localized operation. A distributed trust model has been designed to efficiently defend against the routing attacks. Once trust information is available for all network nodes, the routing decisions can take it into account, i.e. routing can be based on

Table 1. Parameter list

Parameters	Description
Network size	100 nodes
Initial energy	50J per node
MAC Protocol	IEEE 802.15.4
Sensor Node	Imote2
Radio Frequency	13 MHz
Power consumption	Equivalent to packet size and distance
Number of rounds	At least 20

To validate the performance of SEER, a clustered wireless sensor network in a field with dimensions 100 m x 100 m is simulated. The total number of sensor nodes is 100. All the nodes are randomly distributed over the field. Each sensor has its' horizontal and vertical coordinates randomly selected (0 to maximum dimension). The messages sent between the nodes and cluster-heads and also those between the cluster heads and sink node are set to a size of 1KB. The sink is located at any one of the four sides, thus the maximum distance between any node and the sink is approximately 100 m. The initial energy for each node is considered as 50 Joule. The nodes with energy value which is above a threshold value, is known as alive node and that with below threshold value is known as dead node.

The number of dead nodes is obtained after completion of each round. Figure4 traces the rate of increase in the number of dead nodes for 20 rounds. The existing logics SEEM, ATSR and INSENS are also simulated to obtain the number of dead nodes. In case of ATSR, the number of dead nodes after 20 rounds is much less than that of SEEM as it uses geographical location for routing instead of packet exchange to avoid flooding the current state of all network nodes to create a map. Also no weight graph is created for shortest path selection. It is done by calculating trust value which is distributive function of all the nodes. INSENS uses additional routing stage that makes it less energy efficient than ATSR but is better than SEEM. However in SEER, no additional network flooding is required and only trust values are calculated to obtain the path from cluster head to base station. Thus energy consumption will be less than SEEM, ATSR and INSENS. Figure 4 shows this result.

Network lifetime is considered as a parameter to measure the performance of SEER. Network lifetime can be defined as the time span from the deployment to the instant when the network is considered nonfunctional. When a network should be considered nonfunctional is, however, application-specific. It can be, for example, the instant when the first sensor dies, a percentage of sensors die, the network partitions, or the loss of coverage occurs. Figure 6 depicts the performance graph, where the number of sensor nodes or the network size is varying from 30 to 130. Network lifetime means the number of rounds required to loss the coverage of the network. In SEER cluster forms only when some event occurs. Thus with the increase of the network size, the number of clusters will not be increased. Hence in SEER network lifetime is increased significantly with the increase in network size than SEEM, ATSR and INSENS.

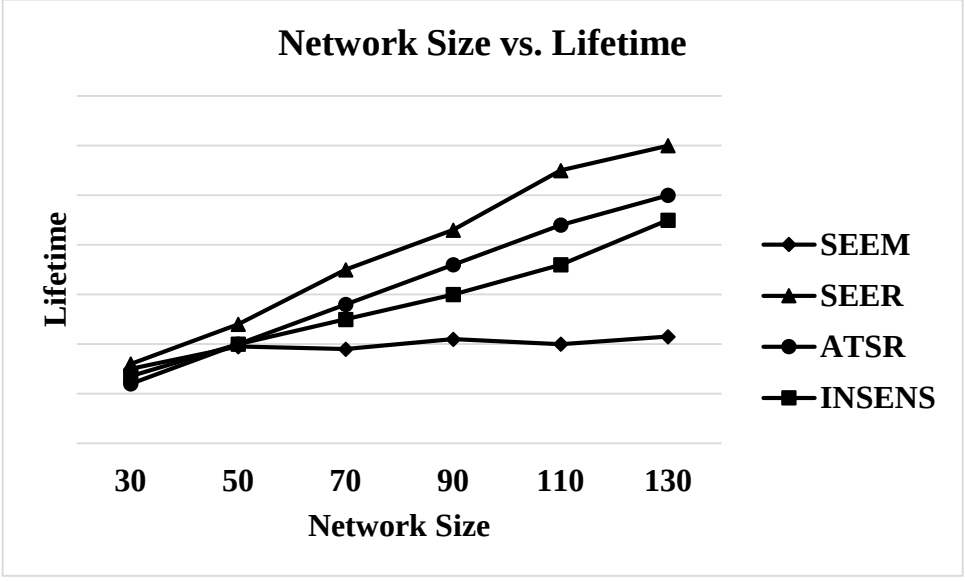

Figure 6. Network size vs. Lifetime

Packet delivery ratio is measured in the presence of malicious nodes. Delivery Ratio can be defined as the ratio of the number of successful packet delivered and the total number of packets sent. In Figure7 number of malicious nodes are increasing from 0 to 50, In SEER, the number of successful packet delivered is highest, among SEEM, ATSR and INSENS. That means SEER increases delivery ratio.

7. Conclusion

In this paper, a brief discussion about energy efficient routing protocols for wireless sensor network have been provided. It is observed that the hierarchical routing protocols have more scopes of balancing the energy utilization than other type of routing protocols. However, security is another criteria that has to be taken care of while sending confidential information through a sensor network. It is a challenging task to take care of both these issues at the same time. The proposed protocol SEER focuses on both energy efficiency and security in wireless sensor network. The event based clustering technique prevents the network from unnecessary cluster making, which leads to a great amount of energy saving. A hash chain based technique with light weight cryptography is used for achieving security as well as reducing the computational overhead. The protocol is able to prevent both external and internal threats. The performance analysis and simulation results show that SEER performs better than other well-known protocols INSENS, ATSR and SEEM.

References

[1] A. Perrig, R. Szewczyk, V. Wen, D. Culler, J. Tygar, Spins: Security protocols for sensor networks, *Wireless Networks Journal (WINET)*, 8 (5), 2002, 521–534.

[2] Asha Rani Mishra and Mahesh Singh, Elliptic Curve Cryptography (ECC) for Security in wireless Sensor Network, *International Journal of Engineering Research & Technology (IJERT)*, Vol. 1 Issue 3, May 2012.

[3] B. Lai, S. Kim, I. Verbauwhede, Scalable session key construction protocol for wireless sensor networks, *IEEE Workshop on Large Scale Real-Time and Embedded Systems (LARTES)*, IEEE Computer Society, Washington, DC, USA, 2002.

[4] C. Cachin, J.A. Poritz, Secure intrusion-tolerant replication on the internet, *IEEE International Conference on Dependable -Systems and Networks (DSN'02)*, Washington DC, USA, June 2002.

[5] C.-F. Law, K.-S. Hung, Y.-K. Kwok, A novel key redistribution scheme for wireless sensor networks, *IEEE International Conference on Communications(ICC'07)*, IEEE Computer Society, Washington, DC, USA, 2007, pp. 3437–3442.

[6] ChakibBekara andMaryline Laurent-Maknavicius, A Secure Aggregation Protocol for Cluster-Based Wireless Sensor Networks with no Requirements for Trusted Aggregator Nodes,*Next Generation Mobile Applications, Services and Technologies, NGMAST7*. 2007.

[7] Chris Karlof and David Wagner, Secure routing in wireless sensor networks: attacks and countermeasures, *Ad Hoc Networks, Elsevier Journal*,doi:10.1016/S1570-8705(03)00008-8, 2003, 293–315.

[8] D. Hwang, B. Lai, I. Verbauwhede, Energy-memory-security trade-offsin distributed sensor networks, *ADHOC-NOW*, Springer, Berlin/Heidelberg, 2004, pp. 7081.

[9] Diffie-hellman, D.Boneh, The Decision Diffe Hellman Problem, *Third Algorithmic Number Theory Symposium*, vol. 1423 of LNCS, Springer,1998.

[10] Ditipriya Sinha, Uma Bhattacharya, Rituparna Chaki, "RSRP: A Robust Secure Routing Protocol in MANET", *in the journal Foundation of Computing and Decision Sciences*, Vol. 39, 2014, No. 2, pp. 129-154, doi: 10.2478/fcds-2014-0008

[25] R. Blom, An optimal class of symmetric key generation systems, *Proceedings of the EUROCRYPT 84 Workshop on Advances in Cryptology: Theory and Application of Cryptographic Techniques*, Springer, New York, USA, 1985, pp. 335–338.
[26] Shamir, A., How to share a secret? *Magazine of Communications of the ACM*, 22, 11, 1979. doi:10.1145/359168.359176
[27] S. Das Bit, R. Ragupathy, "Routing in manet and sensor network – a 3D position based approach", *in the journal Foundation of Computing and Decision Sciences*, Vol. 33, 2008, No. 3, pp. 211-240
[28] T. Shan, C. Liu, Enhancing the key pre-distribution scheme on wireless sensor networks, *IEEE Asia-Pacific Conference on Services Computing*, IEEE Computer Society, Los Alamitos, USA, 2008, pp. 1127–1131.
[29] Varaprasad, G., Dhanalakshmi, S., & Rajaram, M., New Security Algorithm for Mobile Adhoc Networks Using Zonal Routing Protocol. *Ubiquitous Computing and Communication Journal (ubicc.org)*, 2008.
[30] Wang, H., Wu, Z. & Tan, X., A New Secure Authentication Scheme Based Threshold ECDSA For Wireless Sensor Network, in Hamid R. Arabnia & Selim Aissi, ed., Security and Management, *CSREA Press*, 2006, pp. 129-133.
[31] Xukai Zou, Byrav Ramamurthy, Spyros S. Magliveras., Chinese Remainder Theorem Based Hierarchical Access Control for Secure Group Communication, *Third International Conference, ICICS 2001 Xian, China*, Print ISBN: 978-3-540-42880-0, Online ISBN: 978-3-540-45600-1, LNCS series, Series ISSN: 0302-9743, doi: 10.1007/3-540-45600-7_42, vol. 2229, pp.381-385, 2001, Springer.
[32] Y.C. Hu, A. Perrig, D.B. Johnson, Packet leashes: A defence against wormhole attacks in wireless networks, *Proceedings of IEEE Infocom*, April 2003.
[33] Y. Hu, A. Perrig, D. Johnson, Rushing attacks and defence in wireless ad hoc network routing protocols, *Second ACM Workshop on Wireless Security (WiSe'03)*, San Diego, CA, USA, September 2003.
[34] Zhen Cao, Jianbin Hu, Zhong Chen, MaoxingXu, Xia Zhou, FBSR: Feedback based Secure Routing Protocol for Wireless Sensor Networks, *J. PERVASIVE COMPUT. & COMM.*, 1 (1). Troubador Publishing Ltd.
[35] ZigBee Alliance, *Zigbee specification document 053474r06*, v1.0. Technical report, ZigBee Alliance, 2004.

Received 28.11.2014, accepted 28.05.2015