ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105

International Journal on Recent Researches In Science, Engineering & Technology

Volume 5, Issue 3, March 2017.

A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy. It is an absolutely free (No processing charges, No publishing charges etc) Journal Indexed in JIR, DIIF and SJIF.

JIR IF : 2.54
DIIF IF : 1.46
SJIF IF : 1.329

Research Paper
Available online at: www.jrrset.com

ENERGY EFFICIENT ROUTING PROTOCOL FOR SECURE WIRELESS SENSOR NETWORK

A.T.Stephen Thangaraj[1], R.Bavithra[2], J.C.John Charles[2]
[1]Associate Professor, [2,3]Assistant Professor
Department of Computer Science and Engineering
Dhanalakshmi Srinivasan College of Engineering and Technology

Abstract

The ease of deployment of financial sensor networks has always been a boon to catastrophe management applications. However, their vulnerability to a number of security threats makes communication a difficult task. This paper proposes a new routing technique to prevent from both exterior threats and internal threats like good day flooding, eavesdropping and wormhole attack. In this strategy one way hash chain is used to reduce the power drainage. Level primarily based tournament driven clustering also helps to save energy. The simulation effects show that the proposed scheme extends community lifetime even when the cluster primarily based wireless sensor community is below attack.

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

1. Introduction

Wireless sensor networks (WSNs) are hastily developing in their purposes of controlling military activities, health care, home protection and many more. WSN is composed of hundreds, even lots of small sensor nodes, which consists of low cost, restrained strength lifetime, sluggish embedded processors and confined memory. These useful resource limited sensor nodes introduced with one-of-a-kind protection threats, makes WSN extra difficult for the researchers. WSN introduces a mixture of security threats to packet dropping, data altering and jamming. The abilities of an adversary to eavesdrop, tamper with transmitted packets and inject packets to provoke denial-of-service (DOS) attack [7] have been stronger due to the broadcast nature of the wireless conversation medium [18]. The useful resource constraints limit the capability for sensor nodes to operate computation intensive public key cryptography such as RSA [1,16], although elliptic curve cryptography gives a promising direction of lookup [11]. Thus lightweight authentication and encryption approach need to be adopted. Moreover tons superior adversaries outfitted with extra effective computing and conversation tools are in a position to effortlessly inject exterior attacks in opposition to tremendously susceptible defenses of sensor nodes. This leads to physical compromise of one or greater nodes in WSN. Once compromised, the sensor node(s) can be exploited by an intruder to damage the WSN via DOS, jamming, spoofing and numerous different attacks. two two Although, various developments are made in securing the wireless communications, wi-fi sensor community nevertheless faces a range of intricacies with admire to impervious data transmission. Some of the common attacks are sinkhole assault [4], sybil attack [17], wormhole attack [32], speeding attack [33],hello floods assault and selective forwarding [7]. In sinkhole assault a malicious node claims that it has excessive first-rate

route to a vacation spot like base station. The result is countless sensor nodes forwarding their sensed records in the direction of a malicious node. In sybil attack a single node offers a couple of identities to the other nodes. The assault by and large goals multipath routing or geographic routing [19], the place a node accepts a single set of coordinates for each node. Sybil attack creates an illusion that a particular node exists at more than one area at a time. In wormhole attack, an attacker's node is positioned in between two present node of the network. This attacker's node traps all information exchanged between the two current node and promises that to an malicious vacation spot node. In howdy flood attack, a malicious node sends good day messages to a giant variety of nodes in the presence of amazing laptop-class antenna. Those nodes will agree with that malicious node as a neighbor and can acquire messages despatched by using it, which effects in flooding them by way of repetitive messages sent by means of that malicious node. two In speeding attack, a malicious node generates a pretend ROUTE_REQUEST message and makes it attain to other nodes of the network before the proper ROUTE_REQUEST message from a respectable node reaches there. Then these nodes will make the malicious node as its parent. In selective forwarding, a malicious node forwards some packets and drops the others as per its' wish. This makes the other nodes believe it to be an lively node of the community and they ship more messages thru it. However it drops most of the packets obtained and forwards solely a few of them. This paper proposes a tightly closed routing scheme to send the sensed statistics to the base station in an power efficient way. The nodes of the community are divided into distinctive tiers in accordance to their geographic location. The cluster will be shaped when an tournament will take place, as an alternative of making clusters just after deployment of nodes. Thus a excellent quantity of power is saving. Security is every other concern of the paper. Secure Energy Efficient Routing (SEER) protocol for wi-fi sensor community authenticates the nodes with one way hash chain (OHC), observed by using generation of MAC with the help of international key and OHC. OHC is additionally known as one-time password (OTP). The most necessary gain addressed via OTPs is that, in contrast to static passwords, they are not inclined to replay attacks. This ability that a potential intruder who manages to file an OTP that used to be already used to log into a provider or to habits a transaction will now not be capable to abuse it, on account that it will be no longer valid. A second primary benefit is that a node, that uses the identical (or similar) password for more than one neighbors, is not made inclined on all of them, if the password for one of these is won by way of an attacker. A mild weight encryption technique is also proposed to encrypt the sensed data for power restrained sensor nodes. The last part of this paper is organized as follows: Section 2 offers with the assessment of nation of the artwork invulnerable routing topologies. In part three the network framework and threat model is described. Section 4 is the distinctive description of the proposed scheme. In area 5 overall performance analysis is furnished followed via the simulation reviews in part 6. Section 7 is the concluding part 2.

2. Related Work

The safety mechanisms adopted by means of specific hierarchical routing protocols has quite a few execs and cons. To make electricity efficient routing the community has been partitioned into clusters. In [27] the authors have used a 3D function primarily based approach for routing in MANET and WSNs. The complete insurance area is partitioned into a number of cubic structured cells. A proactive routing desk shops telephone statistics as a substitute than node data for decreased size. The supply node exams its' routing table, and forwards the packet in the direction of vacation spot thru the node closest to the destination. In this routing solely a coarse know-how of the dynamic community topology and the full knowledge of the partitions are required. The most of the cluster primarily based protocols did now not reflect onconsideration on safety problems in order to reduce the computational cost. The protocols with some basic protection schemes have been designed to make a stability between invulnerable conversation and energy efficiency. The paper [10] presented a sturdy tightly closed routing protocol primarily based on some basic schemes such as RSA-CRT for encryption and decryption of messages, CRT [31] for protection key generation, Shamir's secret sharing principle [26] for technology of secure routes. Selection of the final route relies upon on the parameters such as battery power, mobility and trust price of the route. The complexity of key generation is decreased to a large extent by using the use of RSA-CRT alternatively of RSA [1,16]. The comparative performance

analysis showed that RSRP outperforms ZRP [29] and SEAD [15]. However the most important drawback of most of the current impenetrable routing protocol is that more stress is given on securing the upstream drift of statistics packets. In many of the algorithms protection demand for the downstream glide of statistics is ignored. Some of the existing routing protocols offer excessive security together with intrusion tolerance however overlooks the energy constraints of the sensor nodes to some extent. However the exceptional sorts of safety schemes are depicted in Figure 1.

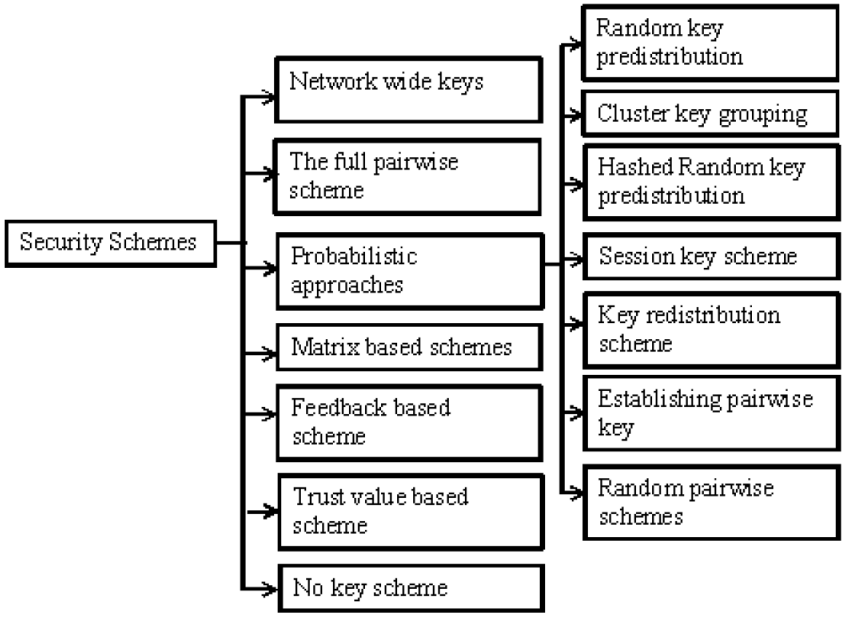

Fig. 1. Different types of security schemes in WSN

2.1. Network large keys

A famous key distribution method is to load a single grasp key into all sensor nodes, which outcomes in a excessive stage of efficiency and flexibility. It requires minimal memory for the storage. The scheme also permits the introduction of any variety of sensors after the preliminary deployment by way of loading the grasp key in new nodes. It gives best key connectivity, on the grounds that all nodes without a doubt share the identical grasp key. An instance of such a safety scheme is the BROadcast Session Key Negotiation Protocol (BROSK) [3]. In this protocol, the grasp key K is used in mixture with random nonce NA and NB, exchanged by using pairs of nodes A and B, for establishing a session key where KA, B = PRF(K||NA||NB), where PRF is a Pseudo-Random Function. In Symmetric-Key Key Establishment (SKKE) [35] scheme, nodes A and B alternate randomly generated challenges NA and NB. The grasp key K is used to compute a common shared secret as SA,B=PRF(K||IDA||B||NA||NB). Then two keys KA, B=Hash(SA,B||1) and K/A,B=Hash(SA,B||2) will be created by SA,B. A tag computed with the aid of K/A,B as TagA=PRF(K/A,B||3||SA,B), is dispatched with the aid of A to B, and TagB=PRF(K/A,B||2||SA,B), is despatched through B to A. This approves the nodes to affirm the computation of the equal hyperlink key KA,B.

twork and their communications will be compromised if the adversary captures a single node and receives the common key. An attacker may also without difficulty insert malicious nodes into the network, once it has get admission to to the master key. two

2.2. The full pair smart scheme

In contrast to the previous schemes used a single grasp key for the verbal exchange between all sensors, in Full Pairwise scheme each of the n nodes in the community receives n1 pairwise keys to communicate with each other node. The node-to-node authentication and perfect resilience is the purpose of high protection in this approach, which prevents node replication attacks. The nodes on the network discover malicious IDs and revoke the corresponding pairwise keys very easily, e.g., by the usage of voting schemes [13,14]. The storing of many keys at each node may additionally motive a exceptional memory overhead. The introduction of new nodes in the community would only be feasible if their keys had been already loaded from the beginning, which turns into a serious restrict when the community desires to be extended over the preliminary expectations. Thus the Full Pairwise

Key scheme could be effectively used essentially in small networks where the maximum range of nodes can be envisioned with proper reliability.

2.3. Probabilistic techniques

In probabilistic approaches, each node receives a group of keys, regarded as key chain, the dimension of which is typically a great deal decrease than the size of the network itself. The main objective of this strategy is to decrease the reminiscence overhead and amplify the safety level. The three awesome and sequential phases on such schemes are Key pre-distribution, shared key discovery and Path-key establishment. The exclusive kind probabilistic tactics are mentioned 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 primary 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 publicizes a list, containing the IDs of all keys in its chain. It approves a neighbor node to become aware of 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, should find an intermediary node C. A suitable candidate will be any node with key chain, which includes key IDs existing 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. two This scheme is used to reduce the amount of reminiscence for storing keys. The scalability and the resilience of the scheme are tremendously structured on the sizes of the key pool and key chains. The drastically high verbal exchange overhead and the lack of node-to-node authentication are the risks of this scheme.

2.3.2. Cluster key grouping

The Cluster Key Grouping [8] scheme proposes a modification to the Random key predistribution scheme. In this approach the key chains are divided into c clusters. Each cluster receives a start key ID. All other IDs in that cluster can be decided with the aid of the start key ID. Thus the broadcasted messages can carry c begin key IDs at the time of Shared-key Discovery phase, while the preceding scheme would require a complete of k≥c IDs. Hence, few IDs are required to be broadcasted for massive clusters. Therefore, this scheme presents communication and reminiscence efficiency with a impervious routing.

2.3.3. Hashed random key pre-distribution

This is some other change to the first probabilistic scheme i.e. Random key predistribution scheme. The Hashed Random Key Pre-distribution (RKP-H) scheme [28] is used to hash the keys from the key pool for distinct nodes. In this solution, solely the first node getting the key Ki from the pool receives and the price of j, while the jth node receives its (j-1) time's hashed version, Hashj-1(Ki). Nodes A and B inform not only the key IDs, but also the price of j for each of them for the duration of the Shared-key Discovery phase. If nodes A and B are loaded, respectively, with KA=Hashja(Ki) and KB=Hashjb(Ki), where (ja>jb), then B can effortlessly compute KA=Hashja-jb(KB). The internet end result of this amendment is that the seize of node C and of its key KC=Hashjc(Ki) will compromise solely the keys KD=Hashjd(Ki) for which jd>jc. Thus the RKP-H scheme trades some storage, communication and computation overhead for more resilience of the secure routing.

2.3.4. Session key scheme

The Session Key Scheme is used to create session keys for each interaction between nodes. The Dynamic Cluster-based Key Management Protocol in Wireless Sensor Networks [21] is based on shared session key. In this protocol the elected cluster head pronounces a hello message to its neighbors, which is authenticated by using an preliminary key. The nodes receiving the message ship an authenticated acknowledgement by means of equal preliminary key to the cluster head together with their ID. The CHs assigns the IDs to every of the nodes that intend to be a part of it and sent the data to the base station. The protocol is primarily based on a symmetric shared session key that is generated the usage of μTESLA [12] protection broadcasting agreement. This is a centralized protocol the place the base station creates the EBS [21] structure and additionally assigns the cluster ID, generates the cluster key and associated administration key which reduces the computation cost of the sensor nodes. The base station encrypts its messages the use of the shared symmetric key and

communicates without delay with the cluster heads only. The gain of this protocol is that there is no want for the cluster head to hold pair keys with cluster nodes. However, familiar communication with the base station increases the overhead of the network.

2.5. Feedback based totally scheme

Feedback Based Secure Routing (FBSR) protocol for Wireless Sensor Networks [34] proposes a routing protocol in which feedback of the contemporary computing ability from neighboring nodes serves as dynamic facts of the cutting-edge network. This helps in selection making of which nodes will take section in the routing in a secured and energy efficient manner. The feedback supplied by way of the neighbors is authenticated with key-one way hash chains developed using µTESLA protocol. The remarks from the base station is utilized to pick out the malicious nodes. Neighbors are selected dynamically and are prioritized on the foundation of their closing 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, primarily based on the feedback value received from the neighbor nodes collectively with their acknowledgement despatched to the sender. This scheme is nicely covered in opposition to sinkhole attack, selective forwarding and sybil attack. However, it is prone to node compromise attack.

2.6. Trust price based totally scheme

Energy-aware Secure Routing for Large Wireless Sensor Networks [24] selects next hop neighbor on the groundwork of last energy of the nodes and their coordinates. Direct and oblique have faith data is also considered. The authors called this method as Ambient Trust Sensor Routing (ATSR). The direct believe cost is evaluated on the basis of a couple of attributes like packet forwarding, network layer acknowledgements, message integrity, node authentication, confidentiality, recognition response, and reputation validation. Monitoring these attributes assist in recognizing various misbehaviors of the nodes and assist in fending off sure attacks. A new node in the network calculates the oblique believe values by way of accumulating the direct have faith values calculated by means of the neighbor nodes. The authenticity of the calculated believe values of the selected nodes depends on their self belief element that will increase with the quantity of interactions of the node with their neighbors. At the time of routing nodes are selected on the basis of trust value, remaining power and distance from the destination.

2.7. No key scheme

Security can also be additionally carried out besides the use of any key. One example of this kind 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 building section is for placing up the network topology; records transmission phase is the working phase, i.e., the sensor network starts offevolved its task; and in route renovation phase, the base station updates on hand energy on every node, participates the communication, and reselects a new route to the supply node. It has three sorts of nodes, such as sensor node, sink node and base station. The base station takes the initiative to discover the multiple paths between the supply nodes and sink node. Three kinds 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 manipulate overhead of the protocol. To comprehend the neighbour nodes of each node, the ND packet is broadcasted in the network. Then the base station declares NC packet in order to acquire the neighbour's records of every node gathered at some stage in the preceding broadcasting. The base station will be stated through the neighbour series reply packet, despatched from sensor nodes.

3. Proposed scheme

The proposed scheme SEER is discussed in 3 extraordinary modules stage formation, cluster formation with impenetrable communication, secure information sensing and aggregation and at closing sending aggregated statistics to the base station.

3.1. Level formation

All the nodes in the network are initialized with a degree value 0 The base station exams the two level fee of the nodes at one hop distance to it, and if they have a degree fee 0, it sets the new level price of those nodes as 1. The nodes with degree fee 1 in flip tests the nodes at 1 hop distance from them. If the newly checked nodes have a degree price 0, then the algorithm will alternate it to 2. This system continues till no nodes are left with degree cost 0

3.2. Cluster formation with secure verbal exchange

In the cluster formation phase, the proposed scheme introduces energy efficiency by way of adopting an event-based cluster formation scheme, where the node that first senses the incidence of an tournament initiates the cluster formation. At first all the nodes of the network calculates a competition bid value (CV) for itself as— CVi=ERi∗Nadj Davg (1) Where for node i, E Ri is the last energy, Nadj is the range of adjoining nodes and Davg is the average distance of node i from all its adjoining nodes. All the nodes that experience the event will be called as Initiator nodes. These Initiator nodes send a control message JOIN to its neighbors. Then every initiator node assessments whether or not its CV value is absolute best among the neighbor Initiator nodes. If it is not very best for any Initiator node then it sends the JOIN message to its neighbor Initiator node, which has the very best CV value. This manner helps the node with absolute best CV fee to get all the sensed records from its neighbor Initiator nodes and it will be declared as cluster head. For example consider Figure2.

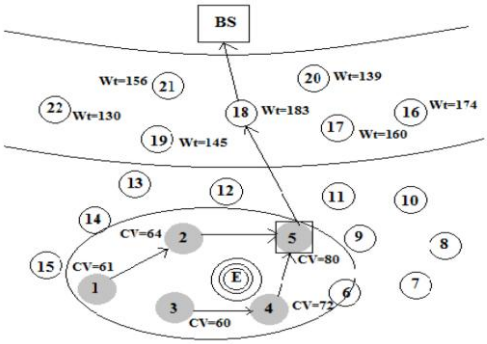

Fig.2 Cluster Formation

In Figure 2 nodes 1,2,3,4 and 5 sensed the same tournament E. All these nodes will be called as Initiator nodes. Node 1 will ship the JOIN message to node 2, as its CV fee is easiest amongst node 1, 2 and 3 Then node three will send the JOIN message to node 4, as it has the absolute best CV fee among all the neighbors of node three Finally node 2 and node four will send their JOIN message to node 5 for the equal reason. That skill node 1 and node 3 will report to node 2 and node four respectively. Both node 2 and node 4 will once more record to node 5, which will take the accountability to send the aggregated records to the base station. Thus a cluster will be fashioned with nodes 1,2,3,4,5 and node 5 will be the cluster head. The thinking is depicted in Fig.3

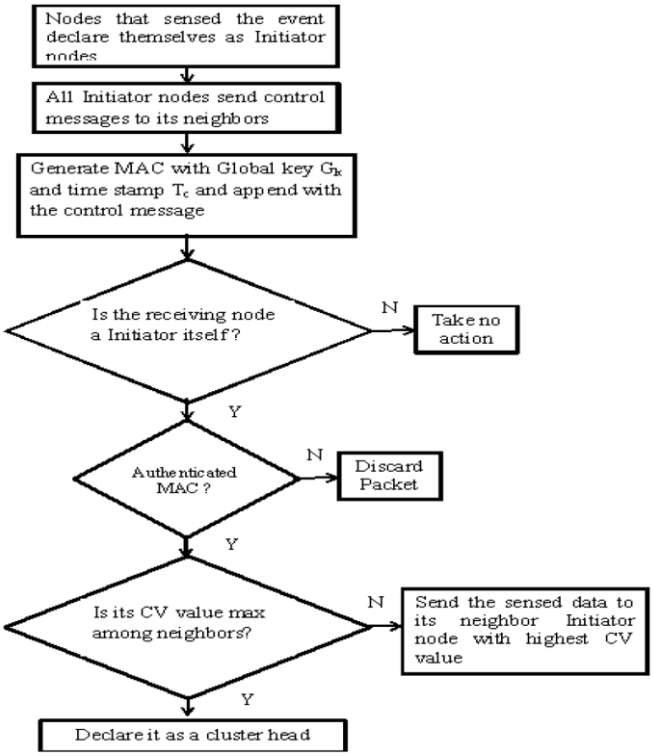

Fig. 3. Flow graph for cluster formation

In SEER, the cluster will be formed solely when an event occurs. The records about that tournament need to be sent to the base station in a very quick time, so that it can take corrective motion as soon as possible. Thus it have to no longer take so an awful lot time to form the cluster.

4. Performance analysis

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

4.1. 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 precept similar to the Client/Server software program architecture. The base station takes the duty of route discovery, renovation and route choice as well. The base station periodically selects a new direction primarily based on present day power degree of nodes. This protocol considers energy-efficiency and security simultaneously. The overall performance analysis indicates that it consequences higher in the concern of throughput, verbal exchange overhead and community lifetime. It also works nicely against some attacks, like Sinkhole attack. In contrast to SEEM, SEER forms the cluster primarily based on the occurrence of events. Though SEER is concerning about safety with energy efficiency like SEEM, the cluster based totally method saves more energy, as in WSN, nodes are deployed very densely and more than one node might also prefer to send the same data about an event. SEEM is unable to face many assaults like wormhole attack, selective forwarding or hello flood attack. SEER may additionally be used to reduce those assaults as it selects the direction relying on have faith fee and power of the nodes, rather of base station is choosing the path. At each move of packets SEER is checking its authenticity with the help of OHC. Simulation consequences show that SEER performs higher than SEEM with recognize to each protection and electricity efficiency. two

4.2. SEER vs. ATSR [24]

A Scalable Geographical Routing method for Wireless Sensor Networks (Ambient Trust Sensor Routing –ATSR) [24] adopts the geographical routing principle which affords high scalability due to its localized operation. A allotted believe model has been designed to efficiently defend against the routing attacks. Once have confidence information is accessible for all community nodes, the routing decisions can take it into account, i.e. routing can be based on both vicinity and believe attributes. It performs higher in phrases of shipping ratio, latency time and course optimality. Though ATSR has used a cluster primarily based method to decrease electricity consumption and designed a trust mannequin for security, it has some problems, which can be solved by using SEER as- a. Trust cost is calculated primarily based on packet rate, acknowledgement, integrity and authenticity, reasons expending more energy. Whereas in SEER it is calculated based on wide variety of packets dropped and energy. b. There is no point out of intra cluster authentication in ATSR. SEER used OHC primarily based MAC authentication scheme to authenticate both cluster heads and cluster member nodes.

4.3. SEER vs. INSENS [18]

Intrusion-tolerant routing for wireless sensor networks (INSENS) [18] securely and efficiently constructs tree-structured routing for wireless sensor networks (WSNs). The key objective is to tolerate damage prompted by using an intruder who has compromised deployed sensor nodes and is intent on injecting, modifying, or blockading packets. To restriction or localize the harm precipitated via such an intruder, INSENS accommodates allotted lightweight security mechanisms, together with environment friendly one-way hash chains and nested keyed message authentication codes that shield against wormhole attacks, as well as multipath routing. Thus INSENS performs higher than ATSR and SEEM. Still it can be accelerated via SEER in some areas as follows- a. INSENS uses three phases: flooding, routing table forwarding and statistics sending. Thus security issue is viewed with an expense of high energy. SEER is a whole lot simplified and strength efficient as it involves solely these nodes which have sensed an tournament and the nodes which are used to ship the information to the base station. b. Data encryption is not executed in INSENS which makes information alteration easier. SEER improves statistics confidentiality by way of a light weight encryption technique, which leads to electricity saving. In INSENS shortest path is chosen using Dijkstra algorithm, and then makes unique sets of nodes to make multiple paths. The technique is very energy and time consuming. SEER calculates weight cost relying on electricity and believe cost to select the next hop node. Thus

sensed information will reach the base station in a brief time with electricity environment friendly secure way.

5. Results & Conclusion

In this paper, a short dialogue about power efficient routing protocols for wireless sensor network have been provided. It is observed that the hierarchical routing protocols have greater scopes of balancing the strength utilization than different kind of routing protocols. However, safety is every other criteria that has to be taken care of while sending confidential statistics thru a sensor network. It is a challenging assignment to take care of both these troubles at the equal time. The proposed protocol SEER focuses on each strength effectivity and safety in wireless sensor network. The event based clustering approach prevents the network from unnecessary cluster making, which leads to a terrific amount of energy saving. A hash chain primarily based method with mild weight cryptography is used for attaining safety as properly as two reducing the computational overhead. The protocol is in a position to forestall each external and interior threats. The overall performance evaluation and simulation outcomes show that SEER performs higher than different prevalent protocols INSENS, ATSR and SEEM.

References

[1] Perrig A., 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] Lai B., 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] Cachin C., 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] Law C. F., 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/S15708705(03)00008-8, 2003, 293–315.

[8] Hwang D., 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-2014-0008Secure

[11] Malan D. J., M. Welsh, M.D. Smith, A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography, First IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks(SECON'04), Santa Clara, CA, USA,October 2004.

[12] Donggang Liu, PengNing, "Multilevel μTESLA: Broadcast authentication for distributed sensor networks", in the journal ACM Transactions on Embedded Computing Systems (TECS), doi>10.1145/1027794.1027800, Volume 3 Issue 4, November 2004, pp. 800-836.

[13] Chan H., A. Perrig, D. Song, Random key pre-distribution schemes for sensor networks, Proceedings of the 2003 IEEE Symposium on Security and Privacy (SP'03), IEEE Computer Society, Washington, DC, USA, 2003, pp. 197–213.
[14] Chan H., V. Gligor, A. Perrig, G. Muralidharan, On the distribution and revocation of cryptographic keys in sensor networks, IEEE Transactions on Dependable and Secure Computing, 2 (3), 2005, pp. 233–247.
[15] Hu, Y. C., Johnson, D. B., & Perrig, A., SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless AdHoc Networks. Ad Hoc Networks Journal Elsevier, 1, 1, 2003, 175-192.
[16] Deng J., R. Han, S. Mishra, The performance evaluation of intrusion-tolerant routing in wireless sensor networks, IEEE 2nd International Workshop on Information Processing in Sensor Networks (IPSN'03), Palo Alto, CA, USA, April 2003.
[17] Douceur J., The sybil attack, First International Workshop on Peer-to-Peer Systems, vol. 2429 of LNCS series, Springer, Berlin, March 2002.
[18] Jing Deng, Richard Han, Shivakant Mishra,INSENS: Intrusion-tolerant routing for wireless sensor networks, Computer Communications, Elsevier,Vol. 29, Issue 2, DOI: 10.1016/j.comcom.2005.05.018,2006, pp.216–230.
[19] Karkazis, P., Leligou, H.C., Orphanoudakis, T., Zahariadis, T., Geographical routing in wireless sensor networks, International conference on Telecommunications and Multimedia (TEMU), IEEE Xplore, E-ISBN: 978-1-4673-2779-4, Print ISBN: 978-14673-2780-0, doi: 10.1109/TEMU.2012.6294717, 2012, pp. 19-24.
[20] Eschenauer L., V. Gligor, A key-management scheme for distributed sensor networks, Proceedings of the Ninth ACM Conference on Computer and Communications Security (CCS'02), ACM, New York, USA, 2002, pp. 41–47.
[21] Lin SHEN and Xiangquan SHI, A Dynamic Cluster-based Key Management Protocol in Wireless Sensor Networks, International Journal Of Intelligent Control And Systems, Vol. 13, NO. 2, June 2008, pp. 146-151.
[22] Nidal Nasser, Yunfeng Chen, SEEM: Secure and energy-efficient multipath routing protocol for wireless sensor networks, Computer Communications, Elsevier,vol. 30, Issues 11–12, DOI: 10.1016/j.comcom.2007.04.014,2007, pp. 2401–2412.
[23] Reza Azarderakhsh, ArashReyhani-Masoleh, and Zine-EddineAbid, A Key Management Scheme for Cluster Based Wireless Sensor Networks, IEEE/IFIP International Conference on Embedded and Ubiquitous Computing,June 2008.
[24] Theodore Zahariadis, Helen C. Leligou, Stamatis Voliotis, Sotiris Maniatis, Panagiotis Trakadas, Panagiotis Karkazis, Energy-aware Secure Routing for Large Wireless Sensor Networks, WSEAS TRANSACTIONS on COMMUNICATIONS, Issue 9, vol. 8, September 2009.
[25] Blom R., 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] Das Bit S., 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] Shan T., 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] Hu Y.C., A. Perrig, D.B. Johnson, Packet leashes: A defence against wormhole attacks in wireless networks, Proceedings of IEEE Infocom, April 2003.
[33] Hu Y., 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.