International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

An Energy Efficient Secure Acknowledgement based Authentication Protocol for WSN

Suman K. Sharma[1], K. T. Jadhao[2]

[1, 2]Alamuri Ratnamala Institute of Engineering and Technology, Department of Electronics and Telecommunication

Abstract: ***Since last few years migration from wired networks to wireless networks is the global trend. This wireless network should be secure and it should have a good lifetime. If the system is not secure or if it does not have a good lifetime, it becomes really costly to maintain wireless network. There are two main functions to enhance the lifetime of a wireless network i.e. clustering and detection of intrusions. We cluster a few nodes to enhance the life efficiency and the node with the highest energy is used for communication. For security, a number of intrusion detection techniques are applied. In this paper we will discuss about multiple clustering and intrusion techniques.***

Keywords: IDS, Clustering

1. Introduction

Traditional wireless sensors have limited energy with large number of static sensor nodes. These sensor nodes are randomly distributed in an area with a limited source of power. Sensor nodes are used to sense the surrounding and this information is then sent to the base station. Efficient use of energy resources and a long life of sensor nodes are must. Most energy of the sensor nodes are in wireless transceiver module.

Multiple techniques have been proposed for energy conservation keeping in mind the data traffic and saving energy. These techniques use flat and hierarchical routing protocols. Based on hierarchical routing protocol, Heinzelman et al. proposed LEACH. LEACH consists of cluster heads, they gather the data and send it to the base station by one hop only. To become the cluster head, each node generates a random number, if the generated random number is less than a certain threshold then the node becomes the cluster head. Cluster heads receive the data from the sensor nodes and transfer it to the base stations. Various other algorithms have been proposed to update the LEACH.

Since the sensor nodes have all the information about the surrounding, it is very prone to get attacked. Hence the security of sensor nodes from intrusions is very important. This data can be used to destroy the wireless network systems. So to prevent the data loss to the intruders various intrusion detection techniques have been proposed.

Firstly, a Watch dog system was proposed, but it was not so efficient so intrusion detection techniques with more successful additions were proposed. Techniques such as ACK, TWOACK, AACK and EAAC were introduced to prevent intrusions and to keep the wireless network system secure. Various clustering algorithms and intrusion detection techniques are described in the following sections.

2. Literature Review

To get a wireless network system that is efficient, has long life and is secure, we need to examine multiple clustering and intrusion detection techniques.

2.1 Clustering Algorithms

The following section consists of algorithms used to increase the life of wireless sensor nodes.

LOWEST ID CLUSTERING (LID) ALGORITHM
LID is a 2-hop clustering algorithm, a node periodically broadcasts a list of nodes that it can hear including itself. Cluster nodes are those nodes which can hear the list of nodes having higher ID than itself from 1-hop neighborhood. A gateway node is one that can hear two or more cluster heads and lies in their transmission range. LID is based on a greedy based algorithm, in this each node consists of a unique identity and the node with the small ID value is assigned as cluster head. LID has the disadvantage of fast battery drainage of the cluster heads.

HIGHEST-CONNECTIVITY (HCN) CLUSTERING ALGORITHM
Nodes having the highest connectivity are termed as the cluster heads. The number of links to 1-hop neighbors is the degree or the connectivity. HCN is purely based on the link cluster algorithm. The throughput is low in HCN algorithm

since HCN incurs higher message overhead because the information about the degree or the connectivity is exchanged.

LIST CLUSTER CHANGE (LCC) ALGORITHM
This is used to minimize the frequency of the cluster heads. The network works properly only if there is cluster stability so LCC is best under such circumstances. The system is robust since the topology of the network changes frequently. LCC has low latency and low routing overhead. The major disadvantage of LCC is unfair distribution of loads amongst the nodes.

WEIGHTED CLUSTERING ALGORITHM (WCA)
The combined weight metric is the bases of the WCA. Various parameters define it such as node speed, node degree, dance with respect to the node neighbor, battery of the node and the time spent as cluster head in the system. The node having the highest weight is termed as the cluster head. This algorithm is good for load balancing. It restricts the number of nodes in the cluster. Since the decision is based on the neighbor, the major disadvantage of this algorithm is the overhead.

LINKED CLUSTER ALGORITHM (LCA)
In LCA, every node should be inside a cluster. All the nodes are organized into a set of cluster nodes. Gateway nodes and cluster nodes are connected providing the global network since the neighbors can access the. If a node has the highest ID value or neighbor has the highest ID value then that node becomes the cluster head. System performance degrades if the cluster nodes are arranged numerically according to their IDs. The major disadvantage of LCA is that the load is not evenly distributed. The LCA also does not take into account the node mobility, adaptive transmission range and power efficiency issues.

LOW-ENERGY ADAPTIVE CLUSTERING HIERARCHY (LEACH)
LEACH is the most energy efficient clustering algorithm. The cluster heads behave like a router for the cluster, the cluster heads are made on the basis of the energy. LEACH is based on the application specific data dimension algorithm. This algorithm increases the system time of operation by using the highest energy node as the cluster. For increasing the life of the nodes, they are randomly shuffled and the load of the nodes also get evenly distributed. LEACH overcomes all the disadvantages of the old protocol.

The clustering terminates within the finite iterations in the LEACH as the nodes are shuffled, so there can be finite number of nodes present in the cluster. It assumes uniform energy consumption of nodes as well as it does not assure good cluster head distribution.

2.2 Intrusion Detection Algorithm

Wireless network consist of both legitimate as well as malicious users, it is very difficult to differentiate between them. Therefore new intrusion detection system of wireless network have been proposed.

WATCHDOG
Watchdog serves as the intrusion detector in the wireless system. This technique helps to improve the output within the presence of malicious nodes. Watchdog detects the presence of malicious nodes by listening to its next hop`s transmission. Watchdog hears that if the next node is not sending the data with the timestamp specified then it increments the failure counter of that node and if the failure counter exceeds the predefined limit then watch dog notifies that the node is misbehaving. Watchdog also maintains a buffer by checking the recently sent packets. It checks if the node is sending the packet or not. The watchdog reports it as misbehaving if the packet is in buffer for too long. Watchdog have disadvantages such as ambiguous collisions, receiver collisions, limited transmission power, false misbehavior report, collusion and partial dropping.

END-TO-END ACKNOWLEDGEMENT SERVICE (ACK)
ACK detects the malicious activity by sending an acknowledgement message to the sender, which says the package has reached successfully. The malicious nodes attract the traffic towards itself but it fails to forward it. Trace route is a protocol which allows the sender to set the tie to live (TTL) of the packet. The router calculates the tie when TTL expires and then sends the warning message to trace route. Then it disguise the message and send it to the routers. The binary search is performed on the routes for efficiency. The weight of the malicious link is increased when it is found so that it cannot be used for future transmission.

TWOACK
The TWOACK system has an authentication mechanism to make sure that the TWOACK packets are genuine. In TWOACK the packets are sent by the receivers for every data packet received from the sender. The TWOACK scheme performs better because it acknowledges fractions of received data packets.

ADAPTIVE ACKNOWLEDGEMENT (AACK)
The AACK is based on TWOACK and ACK. The AACK does not affect the output of the system but reduces the network overhead. Without affecting the output of the system. Here when the sender sends the data packet to the receiver all the nodes in between just forwards to packet to the destination once the receiver receives the packet it will send an ACK to the sender if the sender receives the ACK within the specifies timestamp then only it will state it as successful else will change to TACK. The overhead in the network is greatly reduced because of the hybridization of schemes. When there is a false misbehavior report or a forged acknowledgement packet, TWOACK and AACK fails to detect the malicious nodes since the protocols are very effective.

ENHANCED ADAPTIVE ACKNOWLEDGEMENT (EAACK)
EAACK requires very less amount of hardware, it overcomes the drawbacks of AACK. EAACK uses acknowledgement and timestamp as tools for threat detection. For preventing the attacker to fake the acknowledgement packet, digital signature is also used. The EAACK is divide into three sections, ACK, S-ACK and MRA.EAACK aims at reducing the network overhead and removing the malicious node. Since the transaction is based on the acknowledgement provided by the receiver to the sender, EAACK uses ACK.

In ACK mode, a timestamp is started when the sender sends the message to the receiver. If the acknowledgement packet is not received within the time limit the ACK assumes there is some malicious activity in the network and then the S-ACK detects the threat. For every third consecutive node, the third node will send an S-ACK acknowledgement packet to the first node.

If anything malicious is found out in the S-ACK packet, then MRA mode is initiated and the destination path is changed. To start the MRA mode, the source nodes should first search its local table to find if a new route is possible or not if the new route is possible then the source should check that route and take that route to the destination node. If there is no other route possible, the source node should starts a routing request to find a new route to destination.

3. Implementation

LEACH protocol is divided into phases. Operations are broken into rounds and each round begins with step-up phase where cluster are organized according to the small transmit distance and whether the node wants to be a cluster head or not. Then there is advertisement phase where the decision is made independently, at the same time it is followed by the steady-state phase, when the data is transferred to the base station. In order to minimize the overhead the steady state phase is longer than the step phase.

Set-up phase
Node will become cluster head if, it's energy is highest or second highest, so for becoming cluster head the energy should be,

E1 = Max(Ei),
Where Ei is the energy of each node or

E2 = Max(Ei, where Ei < E1)

Nodes that are cluster head in round 0 cannot become cluster head again. After 1/P-1, T=1 and 1/P rounds, all nodes are eligible again to become cluster heads.

Each node that is elected as a cluster head for the current round broadcasts advertisement messages to rest of the nodes. They use a CSMA MAC protocol. All cluster heads transmit advertisement using same transmit energy. Non cluster head nodes must keep receivers on during this phase to hear advertisements. After phase, they decide which Cluster to belong to for this round by choosing cluster head that requires minimum communication energy. In case of ties, random cluster head is chosen.

Setup to steady phase
After the nodes pick cluster, they must inform the cluster head. It uses CSMA MAC protocol again. Cluster head now knows the number of members and their identifiers after the setup. Cluster head than creates a TDA schedule telling each node when it can transit (Broadcast back to nodes in cluster, probably using CSMA). It allows radio components of each non cluster head node to be turned off during its transit time, thus minimizing energy dissipated in individual sensors. Cluster head now has all the data from the node in its cluster, aggregates data and transmits to base station.

EAACK scheme is implemented with the help of algorithms like DSA and RSA. If the digital signature is used with RSA it can prevent the attackers from forging acknowledgement packet. In EAACK the acknowledgement packets is to be digitally signed before they are sent out and verified until they are accepted and extra resources are required with the introduction of digital signature.

DSA Algorithm

The DSA algorithm procedure can be explained as.

5.1.1 DSA Key Generation

The DSA key generation steps are as follows

Step 1: Firstly shared global public key values (p, q, g) are chosen:
Step 2: Choose a large prime p=2L
Where L=512 to 1024 bits and is a multiple of 64.
Step 3: Choose q,a 160 bit prime factor of p-1
Step 4: Choose g=h(p-1)/q
For any h<p-1, h(p-1)/q(mod p)>1
Step 5: Each user chooses a private key and computes their public key:
Choose x<q,compute y=gx(mod p)

5.1.2 DSA Signature Creation and Verification

The DSA signature creation and verification steps are as follows

Step 1: To sign a message M
Generate random signature key k,k<q compute
- $R=(g^k(\text{mod } p))(\text{mod } q)$
- $S=k^{-1}SHA(M)+x.r(\text{mod } q)$

Send signature (r,s) with message.

Step 2: To verify a signature,compute
- $w= s^{-1}(\text{mod } q)$
- u1=(SHA(M).w)(mod q)
- u2=r.w(mod q)
- v=(gu1.yu2(mod p))(mod q)

if v=r then the signature is verified.

Figure: DSA Algorithm

In DSA the DS is required to verify the sender of a documents identity. The signature is computer using a set of rules and parameters (algorithm) such that the identity of the person signing the document as well as the originality of the data can be verified.

RSA Algorithm

The RSA algorithm steps are as follows.

Step 1: Each user generates a public/private key pair by selecting two large primes at randomp,q
Step 2: Computing their system modulus N=p.q
Where z(N)=(p-1)(q-1)
Step 3: Selecting at random the encryption key e
Where1<e<z(N), gcd(e,z(N))=1
Step 4: Solve following equation to find decryption key d
e.d=1 modz(N) and 0<=d<=N
Step 5: Publish their public encryption key: KU={e,N}
Keep secret private decryption key: KR={d,p, and q}
Step 6: To encrypt a message M the sender:
-obtains public key of recipient KU={e,N}
-Computes: C+Me mod N, where0<=M<N
Step 7: To decrypt the ciper text c:
-uses their private key KR={d,p,q}
-computes: M=Cd mod N

Figure: RSA Algorithm

The algorithm is used in public key cryptography. Based on exponentiation in a finite (Galois) field over integers modulo a prime number. Exponentiation takes O((log n)3) operations. Uses large integers (eg. 1024 bits).Security due to cost of factoring large numbers nb. Factorization takes O (e log n log log n) operations.

4. Result

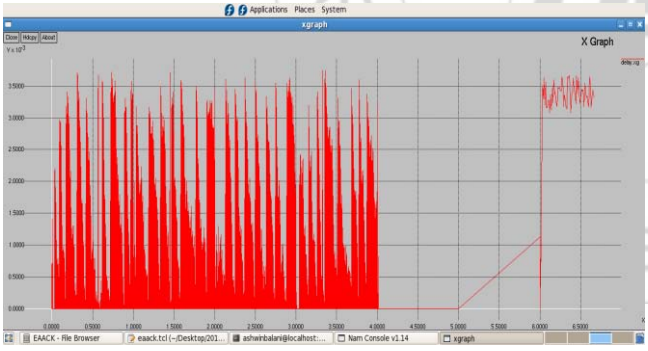

Figure 1: Delay of the system without applying the techniques

The above figure shows the delay of the system when the technique is not applied. In the figure we can observe that delay is nearly 3.5 for 4 seconds. So the Average Delay is more.

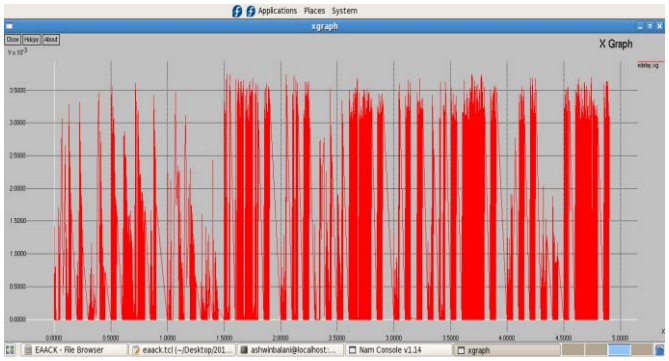

Figure 2: Delay of the system after applying the techniques

In the above figure the delay is same 3.5 but now it is distributed over 5 seconds. Thus the Average delay is comparatively small and the efficiency increases as the delay is lesser then the normal delay.

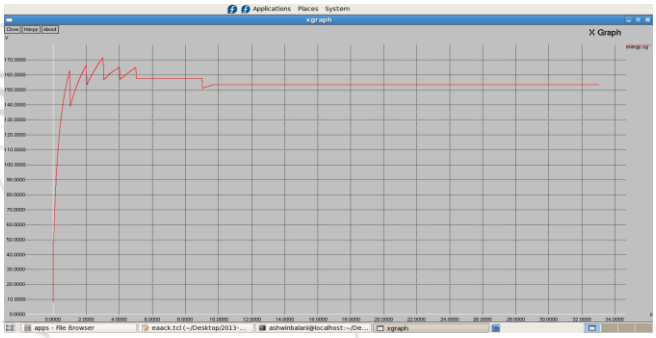

Figure 3: Energy of the system without applying the techniques

When LEACH is not applied the average energy required can be 160, as we can see that in the figure.

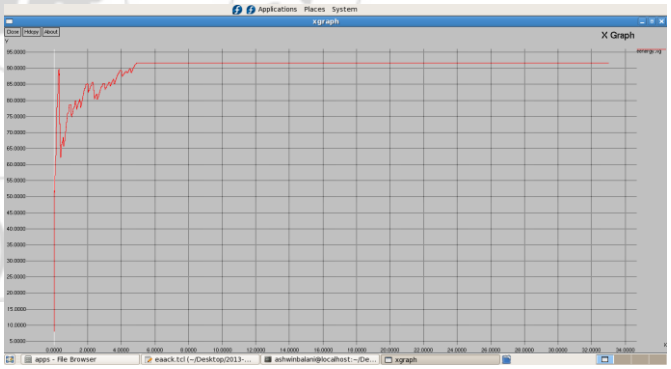

Figure 4: Energy of the system after applying the techniques

The above graph shows the energy reading after the LEACH protocol is applied therefore the average energy required falls from 160 to 90 which is nearly 40% less than the normal scenario.

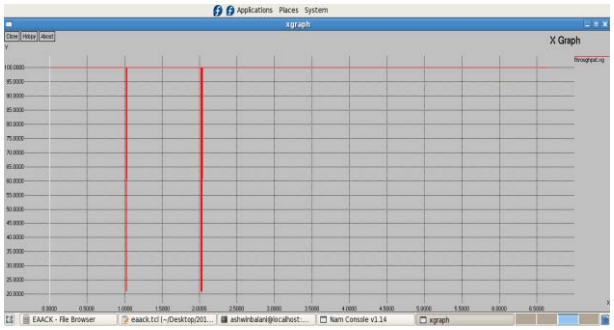

Figure 5: Throughput of the system without applying the techniques

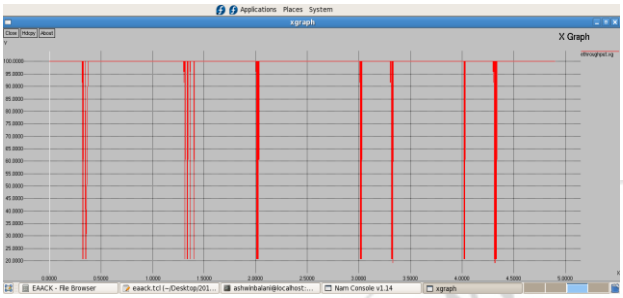

Figure 6: Throughput of the system after applying the techniques

In the above two figures we can see that the throughput is not changing that is the output of the system is same always, just the procedure is optimized.

5. Conclusion

In this paper I showed the implementation of an optimized system. Here the LEACH is used to reduce the power requirement and enhancing the life of the node in the network. Since Wireless is not sufficiently secure we need an authentication mechanism so that the data transfer is secured, for this security we are using EAACK algorithm which increases the security of the system. Here the delay is reduced the energy required is reduced and the desired output is not changed.

Reference

[1] Survey on Intrusion Detection Mechanisms for MANETS by Shwetha M , Mamatha A in IJCSIT 2014
[2] INTRUSION-DETECTION SYSTEM FOR MANETS: A SECURE EAACK by Pratibha Wage, ChannveerPatil in IJRET 2014
[3] A Study On Enhanced Adaptive Acknowledge (EAACK) Scheme in Receiver Collisions – An IDS in Wireless Mobile Ad-Hoc Networks by S. Sujatha, 2, B. Lakshmi Radhika IJES 2013
[4] Energy Efficient Homogenous Clustering Algorithm for Wireless Sensor Networks Shio Kumar Singh 1, M P Singh 2, and D K Singh in IJWMN 2010.
[5] "Intrusion Detection in Wireless Sensor Networks" by Michael Krishnan
[6] "Implementation of EAACK to Detect Node Misbehavior in MANETs using Intrusion Detection Method" by Harshavardhan, Supriya and Shivanand R D.
[7] "Implementation of EAACK Secure Trespass on Detection System for MANETs" by S. Krishna Priya, K. V. Srinivasa Rao.