Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 11, November 2014, pg.699 – 712

RESEARCH ARTICLE

ENERGY AWARE SECURE MULTIPATH ROUTING IN WIRELESS SENSOR NETWORK

Mrs. K.S. Sathyavani*, **Mrs. P. Selvi**, M.Sc., M.Phil.**
*M.Phil(Computer Science), Research Scholar
Vivekanandha College for Women, Unjanai, Tiruchengode, India
****Assistant Professor in Computer Science
Vivekanandha College for Women, Unjanai, Tiruchengode, India

***ABSTRACT:** Secure data transmission is a critical issue for wireless sensor networks (WSNs). Clustering is an effective and practical way to enhance the system performance of WSNs. Cluster routing protocol is used for secure data transmission for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and periodically. CRP uses digital signature (DSI) scheme and the identity-based online/offline digital signature (DSOO) scheme, for security. In DSI security relies on the hardness of the Diffie-Hellman problem in the pairing domain so that it uses the RSA based digital signature hashing technique for signing and verification. In DSOO it reduces the computational overhead for protocol security, which is crucial for WSNs, while its security relies on the hardness of the discrete logarithm problem. Simulation results shows that proposed system has better performance compared with the existing system in terms of security, efficiency, energy consumption.*

***Keywords:** Cluster Head (CH), DSOO, DSI, Digital Signature*

1. INTRODUCTION

A wireless sensor network (WSN) of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

Hierarchical clustering in WSNs can greatly contribute to overall system scalability, lifetime, and energy efficiency. Hierarchical routing is an efficient way to lower energy consumption within a cluster, performing data aggregation and fusion in order decrease the number of transmitted messages to the BS. On the contrary, a single-tier network can cause the gateway to overload with the increase in sensors density. Such overload might cause latency in communication and inadequate tracking of events. In addition, the single-tier architecture is not scalable for a larger set of sensors covering a wider area of interest because the sensors are typically not capable of long-haul communication.

Hierarchical clustering is particularly useful for applications that require scalability to hundreds or thousands of nodes. Scalability in this context implies the need for load balancing and efficient resource utilization.

Cluster formation methodology: In most recent approaches, when CHs are just regular sensors nodes and time efficiency is a primary design criterion, clustering is being performed in a distributed manner without coordination.

2. LITERATURE SURVEY

Barreto Et Al. A several new algorithms to implement pairing-based cryptosystems. The algorithm proposed are practical and lead to significant improvement ,for pairing evaluation process and also helps in the improvement of operation such as elliptic curve scalar multiplication and square root extraction. The goal of the system entirely practical and contribute to fill the theoretical gap in the family of curve and they also propose efficient algorithm for the

arithmetic operation. W. Diffie And M. Hellman. Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems. Yasmin, E. Ritter, And G. Wang. The main contribution of this work is an authentication framework which provides two features; quick authenticated broadcast by sensor nodes and user authentication. Existing broadcast authentication schemes in WSNs do not handle. S. Sharma And S.K. Jena. Routing protocol affects the performance of the network in the form of energy efficiency, security, resiliency and lifetime. So that secure, robust and efficient routing protocol is the basic requirement. S.Even, O. Goldreich, And S. Micali. A new type of signature scheme is used . It consists of two phases. The first phase is performed off-line, before the message to be signed is even known. The second phase is performed on-line, once the message to be signed is known, and is supposed to be very fast. A method for constructing such on-line/off-line signature schemes is presented.

3. PROBLEM DESCRIPITION

3.1 EXISTING SYSTEM

Wireless Sensor networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected. Many data transmission protocols for WSN including the cluster based are vulnerable to number of security attacks. In cluster based protocols since the data aggregation and routing of data depends on CH.so the attacks to the CH can cause serious damage to the network.

Secure data transmission is a critical issue for wireless sensor networks (WSNs). Proposed two secure and efficient data transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the identity-based digital signature (IBS) scheme and the identity-based online/ offline digital signature (IBOOS) scheme, respectively. ID-based encryption (or identity-based encryption (IBE)) is an important primitive of ID-based cryptography. As such it is a type of public-key encryption in which the public key of a user is some unique information about the identity of the user.

3.2 PROPOSED SYSTEM

In the Proposed system clustering and digital signature scheme is implemented for providing energy aware secure multipath routing. Our contribution consists in reducing the control energy for cluster formation by keeping each selected cluster head for more than one transmission round. The proposed algorithm, called Clustering Technique for Wireless Sensor Net-works (CTRWSN) is a self-organizing, dynamic clustering method that divides dynamically, A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document.

Digital signatures employ a type of asymmetric cryptography. For messages sent through a non-secure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender.

A digital signature scheme typically consists of three algorithms: A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.

Various aspects of data transmission in wireless sensors are analyzed . In Learning Phase, rule based learning is analyzed for selecting reliable route and its performance metric is compared with the existing system. Proposed a new protocol scheme DSI is also analyzed for security metric. Finally comparative analysis are made for security, energy-efficiency, performance.

ADVANTAGES:

- Better Confidentiality - Protection from unauthorized persons
- Integrity - consistency of data
- Availability - ensuring access to legitimate users
- Energy-Efficient – less power consumption in order to increase network lifetime.

4. METHODOLOGY

4.1 DIGITAL SIGNATURE

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the

message (authentication and non-repudiation) and that the message was not altered in transit (integrity).

DIGITAL SIGNATURE SCHEME AND IDENTITY BASED ONLINE AND OFFLINE DIGITAL SIGNATURE SCHEME.

DSA - DIGITAL SIGNATURE ALGORITHM

Key generation

Key generation has two phases. The first phase is a choice of algorithm parameters which may be shared between different users of the system, while the second phase computes public and private keys for a single user.

Parameter generation

- Choose an approved cryptographic hash function H. In the original DSS, H was always SHA-1, but the stronger SHA-2 hash functions are approved for use in the current DSS. The hash output may be truncated to the size of a key pair.
- Decide on a key length L and N. This is the primary measure of the cryptographic strength of the key. The original DSS constrained L to be a multiple of 64 between 512 and 1024 (inclusive). NIST 800-57 recommends lengths of 2048 (or 3072) for keys with security lifetimes extending beyond 2010 (or 2030), using correspondingly longer N.[10] FIPS 186-3 specifies L and N length pairs of (1024,160), (2048,224), (2048,256), and (3072,256).[4]
- Choose an N-bit prime q. N must be less than or equal to the hash output length.
- Choose an L-bit prime modulus p such that p–1 is a multiple of q.
- Choose g, a number whose multiplicative order modulo p is q. This may be done by setting g = h(p–1)/q mod p for some arbitrary h (1 < h < p−1), and trying again with a different h if the result comes out as 1. Most choices of h will lead to a usable g; commonly h=2 is used.
- The algorithm parameters (p, q, g) may be shared between different users of the system.

Per-user keys

Given a set of parameters, the second phase computes private and public keys for a single user:

- Choose x by some random method, where $0 < x < q$.
- Calculate $y = g^x \bmod p$.
- Public key is (p, q, g, y). Private key is x.

There exist efficient algorithms for computing the modular exponentiations $h^{(p-1)/q} \bmod p$ and $g^x \bmod p$, such as exponentiation by squaring.

Signing

Let H be the hashing function and m the message:

- Generate a random per-message value k where $0 < k < q$
- Calculate $r = \left(g^k \bmod p\right) \bmod q$
- In the unlikely case that $r = 0$, start again with a different random k
- Calculate $s = k^{-1} \left(H\left(m\right) + xr\right) \bmod q$
- In the unlikely case that $s = 0$, start again with a different random k
- The signature is (r, s)

The first two steps amount to creating a new per-message key. The modular exponentiation here is the most computationally expensive part of the signing operation, and it may be computed before the message hash is known. The modular inverse $k^{-1} \bmod q$ is the second most expensive part, and it may also be computed before the message hash is known. It may be computed using the extended Euclidean algorithm or using Fermat's little theorem as $k^{q-2} \bmod q$.

Verifying

- Reject the signature if $0 < r < q$ or $0 < s < q$ is not satisfied.
- Calculate $w = s^{-1} \bmod q$
- Calculate $u_1 = H\left(m\right) \cdot w \bmod q$
- Calculate $u_2 = r \cdot w \bmod q$
- Calculate $v = \left(\left(g^{u_1} y^{u_2}\right) \bmod p\right) \bmod q$
- The signature is valid if $v = r$

Correctness of the algorithm

The signature scheme is correct in the sense that the verifier will always accept genuine signatures. This can be shown as follows:

First, if g = h(p − 1)/q mod p it follows that gq ≡ hp − 1 ≡ 1 (mod p) by Fermat's little theorem. Since g > 1 and q is prime, g must have order q.

The signer computes

$$s = k^{-1}(H(m) + xr) \bmod q$$

Thus

$$\begin{aligned} k &\equiv H(m)s^{-1} + xrs^{-1} \\ &\equiv H(m)w + xrw \pmod{q} \end{aligned}$$

Since *g* has order *q* (mod p) we have

$$\begin{aligned} g^k &\equiv g^{H(m)w} g^{xrw} \\ &\equiv g^{H(m)w} y^{rw} \\ &\equiv g^{u1} y^{u2} \pmod{p} \end{aligned}$$

Finally, the correctness of DSA follows from

$$\begin{aligned} r &= (g^k \bmod p) \bmod q \\ &= (g^{u1} y^{u2} \bmod p) \bmod q \\ &= v \end{aligned}$$

4.2 ALGORITHM DESCRIPTION

Clustering Algorithm

Algorithm in clustering:

1) Fixed and remote base station

Nodes homogeneous and energy constrained

Radio channel is symmetric

E_A-E_B=E_B-E_A

Sensing rate for all sensors fixed,

CH position rotated among the nodes energy load distributed.

Number of active nodes in the network and the optimal number of clusters assumed a priori

Nodes join a target number of CHs

Node-CH communication-TDMA

2) The below algorithm are used to calculate the transmission energy, denoted as ETx(k, d), required for a k bits message over a distance of d,

ETx(k, d) = ETx_elec(k) + ETx_amp(k, d),

= Eelec * k + ε amp * k * d2.

To receive this message, the energy required is:

ERx(k) = ERx_elec(k) = k * Eelec,

where ETx_elec is the energy dissipation of transmitter electronics and ERx_elec is the energy dissipation of receiver electronics. ETx_amp is the energy of the transmitter amplifier.

Multipath Construction

After the Neighbor Discovery phase, each node possesses their neighbor information and then the Multipath Construction phase starts. We assume that the source node location is known to the sink and based on the location of the source the sink starts the route request process. In this the main concept is that, there are two type of nodes primary and alternate. A node is a primary node if it is in the primary path from source to sink else if it is the part of any alternate path then it is the alternate node. As described in the Algorithm 1, the primary nodes find two paths to the source, the primary path and the alternate path. The primary path is built with the best possible neighbor (having the minimum Location Factor(LF))and the alternate path is constructed with the next best neighbor(having the next minimum Location Factor(LF) after the primary path node).The alternate nodes find one single path towards the source node and searches its neighbor table for the node with minimum Location Factor(LF) and will prefer a primary node if possible, this is done to converge the path else the path can diverge from its direction toward the source.

This Algorithm has two procedures

FindPrimaryPath() andFindAlternatePath()

Which are repeated till the route request reaches the source node.

FindPrimaryPath() : This function is called by both primary and the alternate nodes. If the node is primary node it will broadcast its node type to be primary among its neighbors and search the node with minimum location factor in direction of the source node. In both the above cases the found neighbor nodes can have two possible node types,

1. The node can be a primary node
2. It can be an alternate node

Else it has not been assigned any node type. If the parent node is a primary node then the node type of the found neighbor in any of the above cases will be changed to primary node.

In case the parent node in an alternate node, the node type of the found neighbor will not change if it has already been assigned a node type, and in case it has not been assigned any node type, the node will be assigned as alternate node.

FindAlternatePath(): This function is called only by the Primary nodes for finding an alternate path towards the source. It finds the next best node which is called alternate node and add it in its path.

MULTIPATH ROUTING ALGORITHM

Multipath Construction

Input: Set ofnsensor nodes randomly distributed.

Output:One primary and multiple alternate paths from source to sink.

repeat

if(Node==sinknode)then

FindPrimaryPath();

FindAlternatePath();

else if(node==P rimary)then

FindPrimaryPath();

FindAlternatePath();

else if(node==Alternate)then

FindPrimaryPath();


```
end if
until(node6=Source)
procedure
FindrimaryPath()
if(node==P rimary)then
Broadcast
PRIMARY;
Search for the best node;
node←Primary;
end if
if(node==Alternate)then
Broadcast
ALTERNATE;
Search for the best node and prefer Primary;
if(node6=Primary)then
node←Alternate;
end if
end if
end procedure
procedure
FindAlternatePath()
Ifnode==primarythen
Search for the next best path node accept Primary;
if((node6=P rimary)&&(node6=Alternate))then
node←Alternate;
end if
end if
if(node==Alternate)then
Exit();
end if
end procedure
```


4.3 IMPLEMENTATION TOOL

NETWORK SIMULATOR

These compiled objects are made available to the OTCL interpreter through an OTCL linkage that creates a matching OTcl object for each of the C++ objects and makes the control functions and the configurable variables specified by the C++ object act as member functions and member variables of the corresponding OTcl object. It is also possible to add member functions and variables to a C++ linked OTcl object.

COMPONENTS

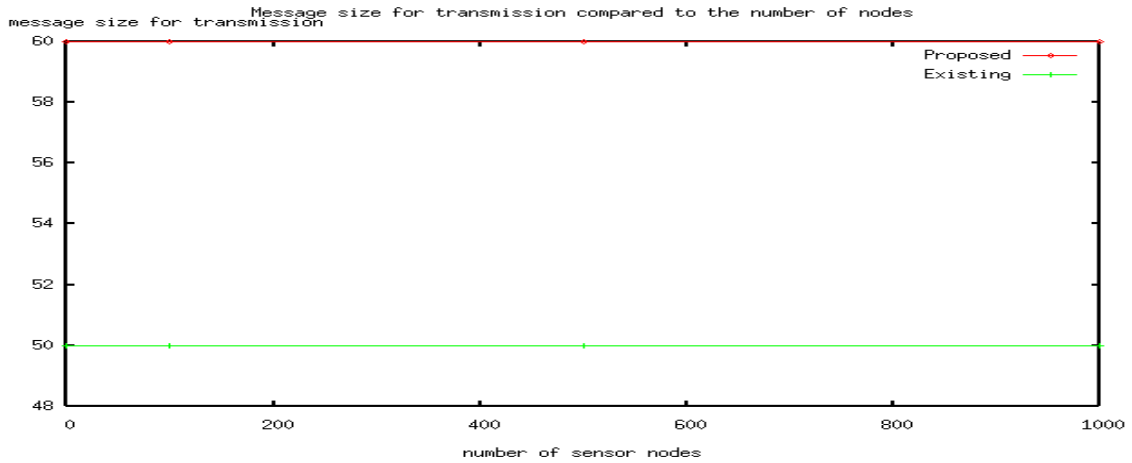
The components used in NS2 are NS- All in one V2.30 Ns is the object oriented TCL (OTCL) Script interpreter that has a simulation event schedule and network component object libraries and network setup module libraries. In other words to use NS you program in OTCL script language. To run the simulation network the user should write an OTCL. Script language that initiated event scheduler and tells network traffic source went to start and stop transmitting package. Another important tool NAM which is used for Network Animation. X-graph tool is used for plotting the NAM log file.

5. EXPERIMENTS AND RESULTS

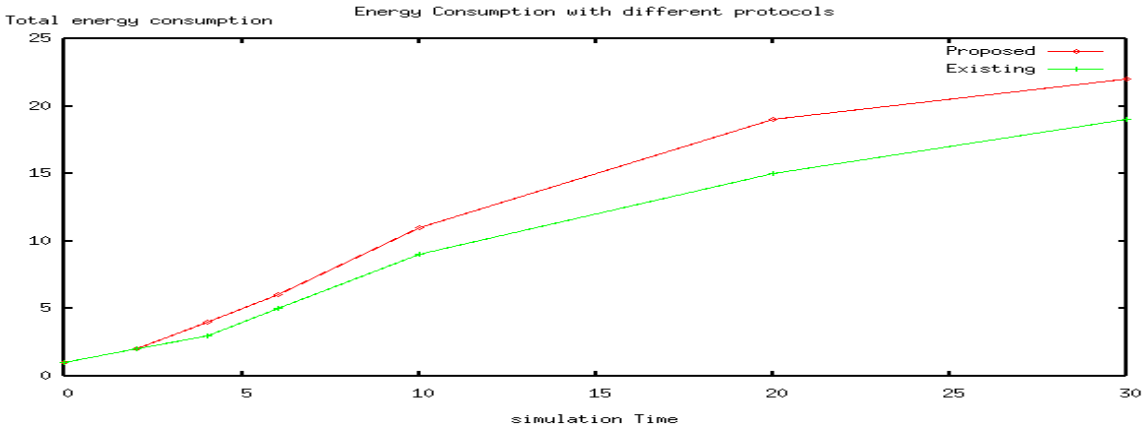
The selected CHs now send advertisement messages in the network declaring their presence as cluster heads. Each node now measures the distance from all the cluster heads. The node joins the CH with minimum distance and sends a message to the nearest cluster head.

Each cluster head is responsible for gathering the data from all the nodes in the cluster. When a frame of data from all the members is received, the CH sends the frame to the base station after applying data aggregation.

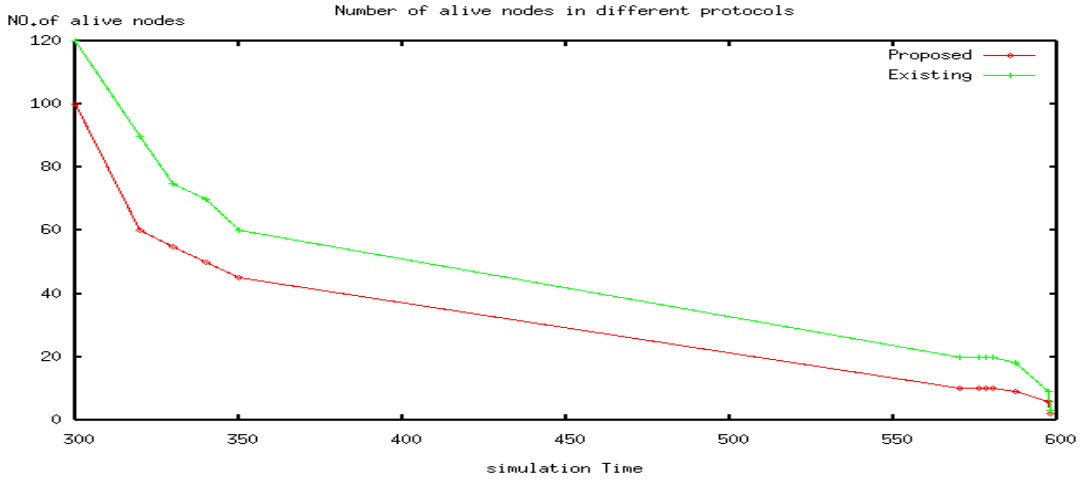
If the size of the cluster is smaller than the predefined threshold, the cluster merges with the neighboring clusters. With the start of the death of nodes, it is found that there are a lesser number of nodes present in each cluster now.



From the above graph, result shows that the total message sizes in different protocols for data transmission. Proposed system has the smallest message size than all the other protocols.



From the above graph, it indicates the balance energy consumption in the network. The results demonstrate that the proposed protocol consume energy faster than existing protocol because of the communication and computational overhead for security .



From the above graph, shown that the comparison of system lifetime using proposed system and existing system. The simulation results demonstrate that the system lifetime of proposed System is longer than that of existing system.

6. CONCLUSION AND FUTURE ENHANCEMENTS

This dissertation proposed a simple, secured and energy-aware protocol for intrusion detection in WSN. This system proposed two secure and efficient data transmission (SET) protocols for CWSNs, called DSI and DSIOO, by using the identity-based digital signature (IBS) scheme and the identity-based online/ offline digital signature (IBOOS) scheme, respectively. Proposed system is to authenticate the encrypted sensed data, by applying digital signatures to message packets, which are efficient in communication and applying the key management for security. To obtain the energy aware system clustering is implemented and cluster heads are elected depends upon the less energy consumption among the group of nodes within the communication range. After cluster head election the nodes are communicated via Cluster Head. Finally comparative analysis is made for security, energy-efficiency, and performance. Simulation results show that energy-aware, secured data transmission with high level of performance achieved in this system.

The proposed system implements energy aware secure routing is implemented. In the proposed system security is given for authentication purpose to communicate the system. But the system doesn't consider for analyzing about the node behaviors. There may be possible the node may be act as a malicious node or adversary node inside the network. So in future, analyze the node behavior and find whether it is a trusted node or not.

REFERENCES

1. T. Hara, V.I. Zadorozhny, and E. Buchmann, **"Wireless Sensor Network Technologies for the Information Explosion Era"**, Studies in Computational Intelligence, vol. 278. Springer-Verlag, 2010.
2. Y. Wang, G. Attebury, and B. Ramamurthy, **"A Survey of Security Issues in Wireless Sensor Networks,"** IEEE Comm. Surveys & Tutorials, vol. 8, no. 2, pp. 2-23, Second Quarter 2006.
3. S. Yi et al., **"PEACH: Power-Efficient and Adaptive Clustering Hierarchy Protocol for Wireless Sensor Networks,"** Computer Comm., vol. 30, nos. 14/15, pp. 2842-2852, 2007.

4. K. Pradeepa, W.R. Anne, and S. Duraisamy, "**Design and Implementation Issues of Clustering in Wireless Sensor Networks,**" Int'l J. Computer Applications, vol. 47, no. 11, pp. 23-28, 2012.
5. L.B. Oliveira et al, **"SecLEACH-On the Security of Clustered Sensor Networks,"** Signal Processing, vol. 87, pp. 2882-2895, 2007.
6. W. Diffie and M. Hellman**, "New Directions in Cryptography,"** IEEE Trans. Information Theory, vol. IT-22, no. 6, pp. 644-654, Nov. 1976.

