ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Resource Conscious Secure routing (RCS) protocol for Wireless Sensor Networks

Dr. S. Senthilkumar and Dr.V.Ravikumar

Maha Barathi Engineering college, chinnaselam 606202

ARTICLE INFO

Article history:
Received 28 January 2015
Accepted 25 February 2015
Available online 6 March 2015

Keywords:
routing, message delivery ratio,energy balance, pattern encoding, random walking

ABSTRACT

Aggravated by the actuality that WSNs routing is often geography based, we propose geography based secure and efficient Resource Conscious Secure routing (RCS) protocol for WSNs without relying on flooding. RCS allows messages to be transmitted using two routing strategies, random walking and deterministic routing, in the same framework. The distribution of these two strategies is determined by the specific security requirements. For security purposes, the content of each message can also be encoded by using pattern encoding method and decoded at the sink node by knowing the swapping bit position. So, unauthenticated person cannot access the original data. By this way, the protocol provides a secure message delivery option to maximize the message delivery ratio under adversarial attacks.

© 2015 AENSI Publisher All rights reserved.

To Cite This Article: Dr. S. Senthilkumar and Dr.V.Ravikumar, Resource Conscious Secure routing (RCS) protocol for Wireless Sensor Networks. ***Aust. J. Basic & Appl. Sci.,*** *9(10): 54-58, 2015*

INTRODUCTION

The wireless sensor networks are currently being used in a wide variety of application ranging from military to civilian applications including monitoring several ambient conditions. A wireless sensor network consists of a collection of many unbound and unattached randomly placed sensor nodes with non-replinishable energy resources. Because of this, routing in wireless sensor networks is a tremendous challenge.

Routing is challenging in wireless sensor networks since it cannot provide soaring message delivery ratio and little energy consumption for message delivery. Routing should also ensure energy balance and security among the sensor nodes thereby extending the sensor network lifetime.

Along with aforesaid issues, wireless sensor networks rely on wireless communication and can be easily attacked by several adversaries due to missing physical boundary. The adversaries can be well equipped and hence they can act upon the network from a distance and extract the messages. They can also cause jamming and traceback attacks.

Propelled by the reality that WSNs routing is often geography based, we propose geography based secure and efficient Resource Conscious Secure routing (RCS) protocol for WSNs without relying on flooding. RCS allows messages to be transmitted using two routing strategies, random walking and deterministic routing, in the same framework. In the Random walking method, there is a chance of choosing low energy node as a relay node. To avoid this, the data is transmitted via energy aware route only, the MES scheme on Elliptic curve algorithm used to provide authentication. For security purposes, the content of each message can also be encoded by using pattern encoding method and decoded at the sink node by knowing the swapping bit position. So, unauthenticated person cannot access the original data. By this way, the protocol provides a secure message delivery option to maximize the message delivery ratio under adversarial attacks.

RCS protocol has two major preferences: (i) Balanced energy consumption can be ensured. (ii) Manifold routing strategies can be used to ensure security. Also, routing traceback attacks and hostile traffic jamming attacks can be detected and prevented.

Related works:

Wireless sensor networks (WSNs) are one of the main widely used in the existing ubiquitous network for various monitoring and tracking applications such as infrastructure monitoring and information collection. Here, confidentiality of the message is ensured using the technique of content encryption, but it is difficult to address the issue of Source-Location Privacy (SLP) of the wireless sensor nodes.

Source Location Privacy is further more complicated by the fact that the wireless sensor nodes generally contain low-cost and low-power radio devices. For this purpose, computationally intensive cryptographic algorithms (such as public-

Corresponding Author: Dr. S. Senthilkumar, Maha Barathi Engineering college, chinnaselam 606202.
E-mail: ssenthilkumar78@yahoo.com

Australian Journal of Basic and Applied Sciences, 9(10) Special 2015, Pages: 54-58

key cryptosystems), and large scale broadcasting-based protocols may not be well suited.

Message authentication has an important role in thwarting unauthorized and corrupted packets from being circulated in networks to save precious sensor energy. For this reason, many schemes have been proposed in literature to provide message authenticity and integrity in network communications.

These schemes can largely be divided into public-key-based and symmetric-key-based approaches.

Earlier, a secret polynomial-based message authentication scheme was introduced to thwart the intruder from recovering the polynomial by computing the coefficients of the polynomial; the idea of adding random noise, called a perturbation factor, to the polynomial was given. But, random noise can be completely removed from the polynomial using error-correcting code techniques.

In sensor networks, the system is divided into grids where each pair of nodes in neighboring grids communicates with each other. In each grid a header node is selected, which coordinates all activities in the grid. Each cell has a unique id and each sensor node knows its relative location through GPS.

Our assumption is that attackers are external, global and precise. We assume that the attackers do not make concessions of any sensor nodes and can monitor the entire traffic in the network. The attackers may perform active attacks such as jamming or any other denial-of-service (dos) attacks.

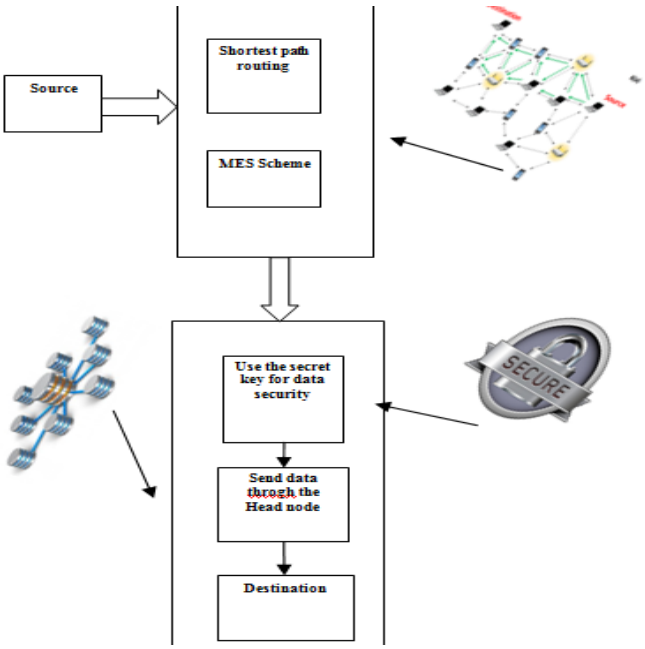
The main idea is that, every node in the network combines valid messages with dummy messages to achieve global security with intervals following constant or probabilistic distribution and source location privacy is preserved even if adversaries conducts various statistical tests.

Flooding provides the least possible privacy protection as it allows the adversary to track and reach source location within the minimum safety period. Baseline flooding and single-path routing cannot provide privacy protection because the adversary can easily identify the shortest path between the source and the sink. This behavior may be considered as a result of the fact that there is a single source in the network and could be easily traced back.

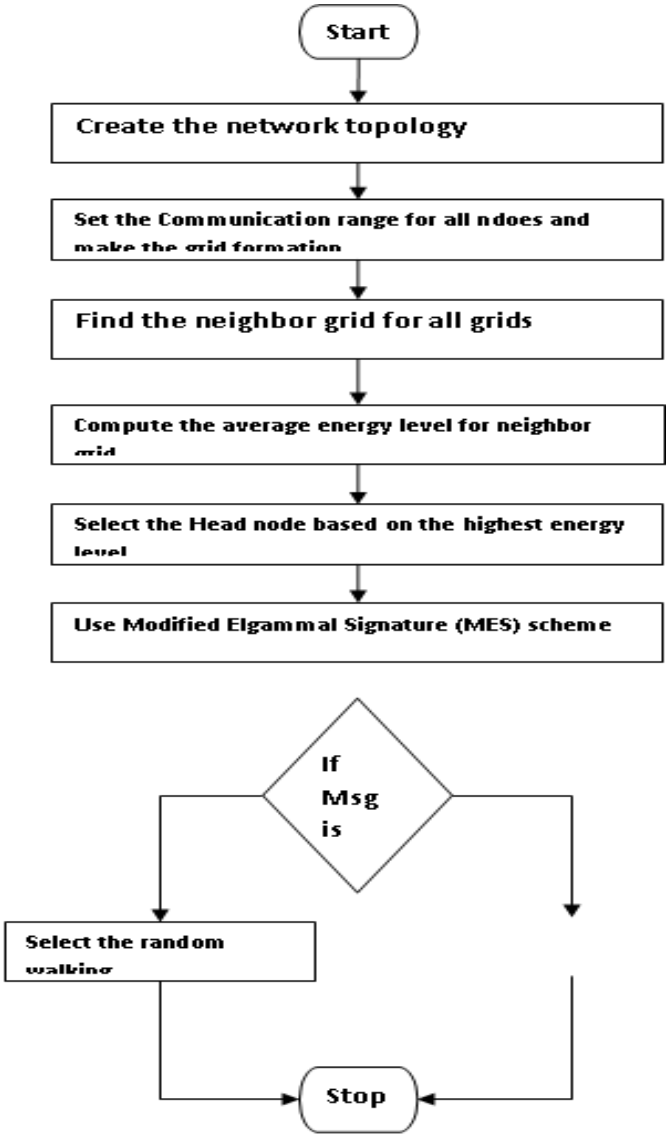
Many new techniques have been devised to enhance source-location privacy in sensor network routing.one of our strategies, called phantom routing, has proven flexible and capable of protecting the source's location, while not a sustainable noticeable increase in energy overhead. Phantom routing techniques yield improved source-location privacy relative to other routing protocols. The basic idea of this method is that once a node decides to become a fake source, it will keep generating fake messages regularly so that attacker may be misled .The main goal behind the phantom techniques is to entice the hunter away from the source towards a phantom source.

System model:

Firstly, we assume that the wireless sensor network is made up of large number of unbound and unattached nodes with a source node and a sink node. The sink node is the final destination node for all the nodes to send the message. Each and every node is given an ID corresponding to its location and energy level. All the nodes are periodically updated of the other nodes energy level and location.



Australian Journal of Basic and Applied Sciences, 9(10) Special 2015, Pages: 54-58



Existing system:

Lifetime optimization and security are two conflicting design issues for multi-hop wireless sensor networks (WSNs) with non-renewable energy resources. In this paper, they proposed a novel secure and efficient Cost-Aware Secure Routing protocol to address these two conflicting issues through two adjustable parameters: energy balance control and probabilistic-based random walking. They then discovered that the energy consumption is severely disproportional to the uniform energy deployment for the given network topology, which greatly reduces the lifetime of the sensor networks. To solve this problem, they proposed an efficient non-uniform energy deployment strategy to optimize the lifetime and message delivery ratio under the same energy resource and security requirement.

Proposed system:

In our paper, the network is equally divided into little grids. Each grid has a relative location based on the grid information. The node in each grid with the greater energy level is selected as the head node for message forwarding. The head node can be reelected if the energy level becomes low than other nodes in the grid. In addition, each node in the grid will maintain its own attributes, including location information, remaining energy level of its grid, as well as the attributes of its adjacent neighboring grids.

The information maintained by each sensor node will be updated periodically. In this project, we will focus on two routing strategies for message forwarding: shortest path message forwarding, and secure message forwarding through random walking to create routing path unpredictability for source privacy and jamming prevention.

To avoid the storage of secret keys we are going to use pattern encoding for encoding and decoding purpose.

Pattern encoding:

In Pattern Encoding, the bits in the binary stream of the data that is sent by the sender are swapped and

Australian Journal of Basic and Applied Sciences, 9(10) Special 2015, Pages: 54-58

a map is attached to the data that is being sent to the receiver. The receiver re-arranges the bits in the binary stream and reads it. The hacker who gets this data converts the binary stream to English alphabets without re-arranging leading to receiving the wrong information.

Mes scheme:

MES scheme on Elliptic curve algorithm

Let p > 3 is an odd prime. An elliptic curve E is defined by an equation of the form:

$E : y^2 = x^3 + ac + b \ mod \ p,$

Where a, b$\in F_p$, and $4a^3 + 27b^2 \not\equiv 0 \ mod \ p.$ The set E(F_p) consists of all points (x,y) $\in F_p$on the curve, together with a special point O, called the point at infinity.

Let G = (x_G,y_G) be a base point on E (F_p) whose order is a very large value N. user A selects a random integer $d_A \epsilon$[1, N-1] as his private key. Then, he can compute his public key $Q_A$from$Q_A = d_A \times G$.

Signature generation algorithm:

For Alice to sign a message m, she follows these steps:

1. Select a random integer k_A,1$\leq k_A \leq N-1$.
2. Calculate r = $x_A mod$ N, Where (x_A,y_A) = k_A G. If r = 0, go back to step 1.
3. Calculate$h_A \overset{l}{\leftarrow} h(m,r)$, where h is a cryptographic hash function, such as SHA-1, and $\overset{l}{\leftarrow}$ denotes the l leftmost bits of the hash.
4. Calculate s = r$d_A h_A + k_A$mod N. If s =0, go back to step 2.
5. The signature is the pair (r,s).

Signature verification algorithm:

For Bob to authenticate Alice's signature, he must have a copy of her public key $Q_A$then he:

1. Checks that $Q_A \neq$O, otherwise invalid
2. Checks that Q_A lies on the curve
3. Checks that $nQ_A = O$

After that, Bob follows these steps to verify the signature:

1. Verify that r and s are integers in [1, N – 1]. If not, the signature is invalid.
2. Calculate $h_A \overset{l}{\leftarrow} h(m,r)$, where h is the same fucntion used in the signature generation.
3. Calculate (x_1,x_2) = sG - r$h_A Q_A$mod N.
4. The signature is valid if r = x_1 mod N, invalid otherwise.

Algorithm:

The algorithm for the proposed system:

Input: Node energy level (NEL) , Neighbor Grid (NG), Base point, threshold

Output: route, Message Signature

Threshold_ energy→Transmission power

Ng →No. of grids

For all grids ng

For each node in grid ng

GH→ node with highest energy level (NEL)

End for each End for

//Shortest path routing

i→source grid j→destination grid

if (i==j) { //Directly transmit the data vis GH

} else { Set route GH(i)

While (Destination reached ==true)

For each node in NG (i)

If {NG(i)==j}

Append route GH(NG(i))

Destination reached→true

End if

Else

Append route GH(NG(i))

Destination reached→false

End for each

End while

// Hop by Hop Authentication

//Signature Generation

1. Select a random integer k_A,1$\leq k_A \leq N-1$.
2. Calculate r = $x_A mod$ N, Where (x_A,y_A) = k_A G. If r = 0, go back to step 1.
3. Calculate$h_A \overset{l}{\leftarrow} h(m,r)$, where h is a cryptographic hash function, such as SHA-1, and $\overset{l}{\leftarrow}$ denotes the l leftmost bits of the hash.
4. Calculate s = r$d_A h_A + k_A$mod N. If s =0, go back to step 2.
5. The signature is the pair (r,s).

//Signature Verification

Verify that r and s are integers in [1, N – 1]. If not, the signature is invalid.

2. Calculate $h_A \overset{l}{\leftarrow} h(m,r)$, where h is the same fucntion used in the signature generation.
3. Calculate (x_1,x_2) = sG - r$h_A Q_A$mod N.
4. The signature is valid if r = x_1 mod N, invalid otherwise.

//Grid Head Reelection

For all the Grids I

If (NEL(GH(i)) <threshold_energy)

Set GH(i) →Node with highest energy

End if End for

Conclusion:

Thus, the proposed system of combining the deterministic shortest path algorithm with high energy balance and MES Elliptic curve cryptographic algorithm can provide highly secure message transfer from source to node and also the pattern encoding method ensures authentication of the message.

REFERENCES

Hung, C.C., K.J. Lin, C.C. Hsu, C.F. Chou and C.J. Tu, 2010. "On enhancing network-lifetime using opportunistic routing in wireless sensor networks," in Computer Communications and Networks (ICCCN), 2010 Proceedings of 19th International Conference on, Aug.

Li, Y., J. Li, J. Ren and J. Wu, 2012. "Providing hop-by-hop authentication and source privacy in wireless sensor networks," in IEEE INFOCOM 2012 Mini-Conference, Orlando, Florida, USA., March 25-30.

Li, Y., Y. Yang and X. Lu, 2010. "Rules of designing routing metrics for greedy, face, and combined greedy-face routing," Mobile Computing, IEEE Transactions on, 9(4): 582–595.

Liu, F., C.Y. Tsui and Y.J. Zhang, 2010. "Joint routing and sleep scheduling for lifetime maximization of wireless sensor networks," Wireless communications, IEEE Transactions on, 9(7): 2258–2267.

Source-location privacy through dynamic routing in wireless sensor networks, 2010. "In Proceedings of IEEE INFOCOM 2010, San Diego, USA., March 15-19.