Volume No:2, Issue No:3 (August-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Enhanced Cost-Aware Position verification Security Routing Protocol Design for WSN

Madem Puneetha
M.Tech,
Dept of CSE,
Vignana Bharathi Institute of Technology,
Proddatur, Kadapa.

K.Vijaya Bhaskar Reddy
Assistant Professor,
Dept of CSE,
Vignana Bharathi Institute of Technology,
Proddatur, Kadapa.

Abstract:
The main objective of this project is to provide the security and increase the network life time. We selected our domain energy management in wireless sensor networks to improve the security system. A typical wireless sensor network consists of several tiny and low-power sensors which use radio frequencies to perform distributed sensing tasks. These nodes often have very limited and non-replenish able energy resources, which makes energy an important design issue for these networks. Routing is another very challenging design issue for WSNs. A properly designed routing protocol should not only ensure high message delivery ratio and low energy consumption for message delivery, but also balance the entire sensor network energy consumption, and thereby extend the sensor network lifetime. In this project, we presented a secure and efficient Cost Aware Secure Routing protocol for WSNs to balance the energy consumption and increase network lifetime. Further we enhance the base work to avoid the fake position indicator nodes by using the distance parameters.

Keywords: Wireless sensor network, Security, Energy efficiency, Geo Routing

1.Introduction:
Future sensor networks will be composed of a large number of densely deployed sensors nodes. Each node in the sensor network may consist of one or more sensors, a low power radio, portable power supply, and possibly localization hardware, such as a GPS (Global Positioning System) unit or a ranging device. A key feature of such networks is that their nodes are unattended.Consequently, they have limited and non-replicable energy resources. Therefore, energy efficiency is an important design consideration for these networks. In this paper we study energy efficient geographic packet forwarding techniques. Disseminating information to a geographic region is a very useful primitive in many location aware systems, and especially sensor networks. The region can be expressed, for example, by a rectangle in 2-space. In order to fulfill the above communication task, this query needs to be disseminated to the sensors in the specified region. An efficient way to disseminate the geographic query to a specified region is to leverage the location knowledge in the query and to route the query directly to the region instead of flooding it everywhere. Previous research has studied how to geographically route a packet to a target location in an ad-hoc network. Sensor networks rely on wireless communication, which is by nature a broadcast medium and is more vulnerable to security attacks than its wired counterpart due to lack of a physical boundary.

In the wireless sensor domain, anybody with an appropriate wireless receiver can monitor and intercept the sensor network communications. The adversaries may use expensive radio transceivers, powerful workstations, and interact with the network from a distance since they are not restricted to using sensor network hardware. It is possible for the adversaries to identify the message source or even identify the source location, even if strong data encryption is utilized. Source-location privacy (SLP) is an important security issue. Lack of SLP can expose significant information about the traffic carried on the network and the physical world entities. While confidentiality of the message can be ensured through content encryption, it is much more difficult to adequately address the SLP. Preserving SLP is even more challenging in WSNs

Volume No:2, Issue No:3 (August-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

since the sensor nodes consist of only low-cost and low-power radio devices, and are designed to operate unattended for long periods of time. Battery recharging or replacement may be infeasible or impossible. Computationally intensive cryptographic algorithms, such as public-key cryptosystems, and large scale broadcasting based protocols, are not suitable for WSNs. To optimize the sensor nodes for the limited node capabilities and the application specific nature of the WSNs, traditionally, security requirements were largely ignored.This leaves WSNs vulnerable to network security attacks. In the worst case, adversaries may be able to undetectably take control of some wireless sensor nodes, compromise the cryptographic keys, and reprogram the wireless sensor nodes. In this paper, we first propose some criteria to quantitatively measure source-location information leakage for routing-based SLP schemes.

Through the proposed measurement criteria, we are able to identify security vulnerabilities of some exiting SLP schemes. We then propose a scheme that can provide both content confidentiality and SLP through a two-phase routing. In the first routing phase, the message source randomly selects an intermediate node in the sensor domain and then transmits the message to the randomly selected intermediate node (RSIN). This phase provides SLP with a high local degree. In the second routing phase, the messages will be routed to a ring node where the messages will be blended through a network mixing ring (NMR). By integrating the NMR, we can dramatically decrease the local degree and increase the SLP. Our simulation results demonstrate that the proposed scheme is very efficient and can achieve a high message delivery ratio. We believe it can be used in many practical applications.

2.Related work:

The main ideas of [1] authors approach were to eliminate the unidirectional link at the network layer and design novel handshake and channel reservation mechanisms at the medium-access control layer u sing topological information collected in the network layer. This paper only to detect the unidirectional links and to avoid the transmissions based on asymmetric links without considering the benefits from high-power nodes. In [2] paper, author proposed a cross layer framework that effectively improves the performance of the MAC layer in power heterogeneous ad hoc networks. In addition, our approach seamlessly supports the identification and usage of unidirectional links at the routing layer. In [3] paper author considered the periodic hello sharing is to find the unidirectional link. But this periodic sharing may be causes to overhead in the network. In [4] paper, author proposed a distributed solution based on reducing the density of the network using two mechanisms: clustering and adjustable transmission range. By using adjustable transmission range, author also achieved another objective, energy efficient design, as a by-product. In [5] paper, author considered clustering mechanism. Due to tightly coupled technique may increase the delay in data transmission. In [5] paper, author presents ad-hoc on demand distance vector routing (AODV), a novel algorithm for the operation of such ad-hoc networks. Each mobile host operates as a specialized router, and routes are obtained as needed (i.e., on-demand) with little or no reliance on periodic advertisements.

AODV is an on demand routing protocol in which routes are established on demand and destination sequence numbers are used to find the latest route to the destination. The connection setup delay is less. The hello messages supporting the routes maintenance are range-limited, so they do not cause unnecessary overhead in the network but the intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence number, thereby having stale entries. In [6] paper, author presents a mathematical framework for quantifying the overhead of proactive routing protocols in mobile ad hoc networks. He focus on situations where the nodes are randomly moving around but the wireless transmissions can be decoded reliably, when nodes are within communication range of each other.

2.1.Existing system summary:

Several geographical routing protocols have been proposed in recent years for wireless sensor networks. In geographical routing each node forwards messages to its neighboring nodes based on estimated cost and learning cost. The estimated cost considers both the distance to the destination and the remaining energy of the sensor nodes. Source location privacy is provided through broadcasting that mixes valid messages with the dummy messages not only consumes the significant of sensor energy but also increases the network collisions and decrease the packet delivery ratio.

Volume No:2, Issue No:3 (August-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

3. Proposed system:

We discover 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, we propose a secure and efficient Cost-Aware Secure Routing protocol that can address energy balance and routing security concurrently in WSNs. In CASER protocol, each sensor node needs to maintain the energy levels of its immediate adjacent neighboring grids in addition to their relative locations. 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.

3.1. Route discovery:

Initially all node collecting the data about neighbor nodes, the network monitors having the detailed information of neighbor nodes such as routing table, It provides the connection information to route manager.

3.2. Energy updating:

The mobile devices periodically share their residual energy into all the nodes which are participating in the network. Based on this energy nodes will select the route in reliable.

3.3. Calculating hop-by-hop energy:

When source node sends rreq, nodes will check the energy of all its one hop neighbor nodes. Then the node select the next node which one has high energy cost. All the nodes do the same process.

3.4. Neighbor processing:

This module is divided into two sub modules named as 1) Poll Process and Data process

-- Poll Process

– By using this module the node can verify the neighbors.

3.5.Data Process

In this sub module, the node has to cross check the database. Ex, if node wants to verify the node x, then the verifier checks the database (which is collected from the neighbor). In this checking process verifiers compares the distance b/w each neighbor and node x

The distance is calculated in two ways

- Location based comparison
- Data transmitted speed comparison

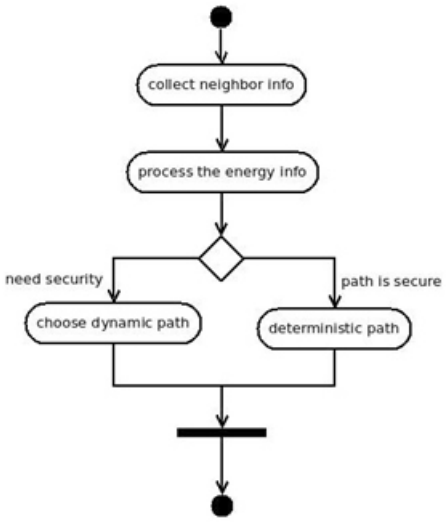


Fig.1 activity of proposed model

Results:

To simulate our proposed work we need Single PC with 20 Gb Hard disc space, 1GB RAM and software is Linux OS (Ubuntu 10.04) and NS2.34. We used the programming languages: TCL , C++ (Optional). Fig. R1 shows the network placement.

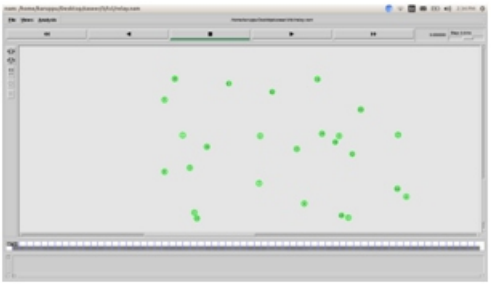


Fig.R1 Network placement

Fig. R2 shows the results of route discovery.

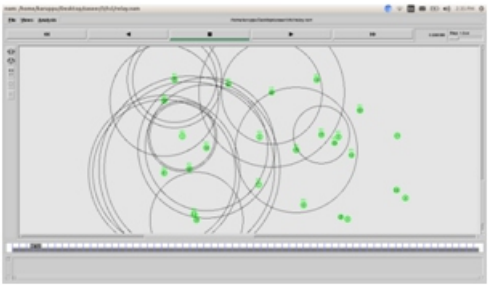
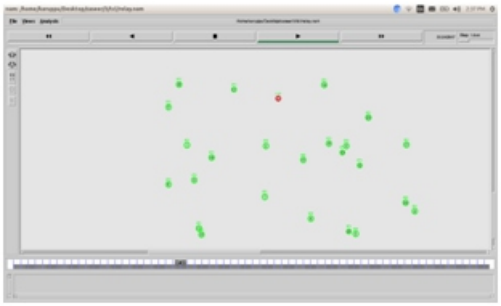


Fig.R2 route discovery

Volume No:2, Issue No:3 (August-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Fig. R3 shows the result of node failure



FigR3 node failure

Fig.R4 and R5 shows the attacker which is trying to track the source location

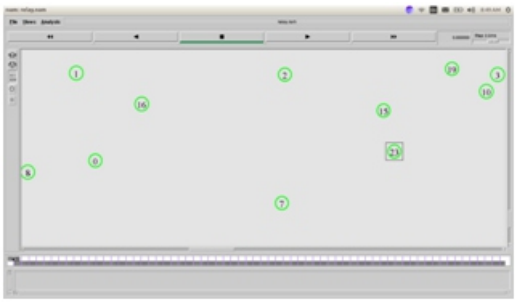


Fig.R4 attacker movement

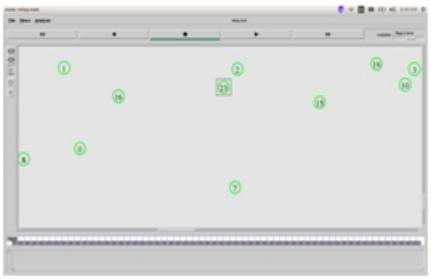


Fig.R5 attacker movement

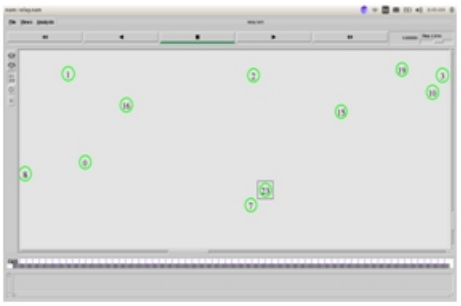


Fig.5 attacker fails to find the source

Fig.R6 shows the comparison of life time for existing, proposed and enhancement.

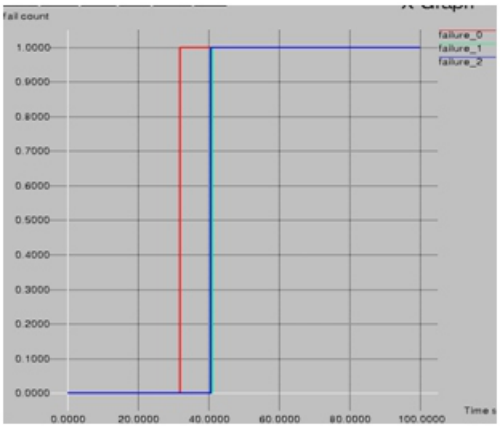


Fig.R6 Energy efficiency graph

Fig.R7 shows the result of PDF comparison

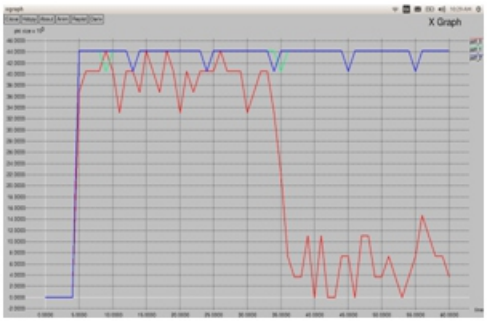


Fig.R7 PDF

Conclusion:

In this project, we presented a secure and efficient Cost Aware Secure Routing protocol for WSNs to balance the energy consumption and increase network lifetime. Further we enhance the base work to avoid the fake position indicator nodes by using the distance parameters.

Reference:

1)Y. Huang, x. Yang, s. Yang, w. Yu, and x. Fu, "cross-layer approach asymmetry for wireless mesh access networks", mar. 2011.

2)V. Shah, e. Gelal, and p. Krishnamurthy, "handling asymmetry in power heterogeneous ad hoc networks: a cross layer approach", jul. 2007.

3)J. Wu and f. Dai, "virtual backbone construction in MANET's using adjustable transmission ranges", sep. 2006

Volume No:2, Issue No:3 (August-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

4)Ad-hoc on-demand distance vector routing----> charles e. Perkins, elizabeth m. Royer.

5)Routing overhead as a function of node mobility: modeling framework and implications on proactive routing-->xianren wu, hamid r. Sadjadpour and j.j.garcia-luna-aceves.

6)Survey of routing protocols in mobile ad-hoc networ----> kevin c. Lee, uichin lee and mario gerla.

Author's Details:

Madem Puneetha received B.Tech (CSE) from JNTUH and pursuing M.Tech (CSE) Vignana Bharathi Institute of Technology, Proddatur, Kadapa Dist from JNTU Anantapur.

K.Vijaya Bhaskar Reddy received B.Tech (CSE) from JNTUH and M. Tech (CSE) degree from JNTUK . He possessed a decade of experience and expertise in Teaching, Training, Industrial and entrepreneurship. Technical expertise includes Cloud Computing, UNIX/ Linux Administration and Compiler Design.Presently he is working as Assistant Professor in Vignana Bharathi Institute of Technology, Proddatur, Kadapa Dist.