IJDCST @Aug-Sept-2015, Issue- V-3, I-6, SW-10
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Improved Secure Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks Using Distributed Coordinating Solution

P.Swetha[1] , K.Sri Lakshmi[2]
M.Tech[1] ,swethaporeddy13@gmail.com[1]
Assistant Professor[2], krovvidisrilakshmi@gmail.com[2]
Dept of Information Technology[1, 2]
G.Narayanamma Institute of Technology Hyderabad, Telangana, India.[1, 2]

Abstract: The development of ad hoc networking protocols and position-aware services require that mobile nodes learn the position of their neighbors. However, such a process can be easily abused or attacked by adversarial devices. In absence of a-priori legitimate nodes, the finding and checking of neighbor positions presents challenges that have been rarely investigated in the literature. In our base paper work, the researchers addressed this open issue by proposing a distributed coordinating solution that is strong against independent and group adversaries, and in our enhancement work we address the energy based adversary attack.

Key word: MANET, Attacker, Position based routing, energy based routing.

I. Introduction:

Emerging wireless networking and mobile computing technologies offer a new rich set of tools, they also open the door to new vulnerabilities, primarily because wireless communication makes eavesdropping and injection of messages easy. Realizing that attacks against a wireless system can be perpetrated essentially anywhere and anytime, the research community devised a large volume of solutions to secure wireless networking protocols and applications. Location awareness has become an asset in mobile systems, where a wide range of protocols and applications require knowledge of the position of the participating nodes. Geo-graphic routing in spontaneous networks, data gathering in sensor networks, movement coordination among autonomous robotic nodes, location-specific services for hand-held devices, and danger warning or traffic monitoring in vehicular networks are all examples of services that build on the availability of neighbor position information.

The correctness of node locations is therefore an all-important issue in mobile networks, and it becomes particularly challenging in the presence of adversaries aiming at harming the system. In these cases, we need solutions that let nodes (1) correctly establish their location in spite of attacks feeding false location information, and (2) verify the positions of their neighbors, so as to detect adversarial nodes announcing false locations.

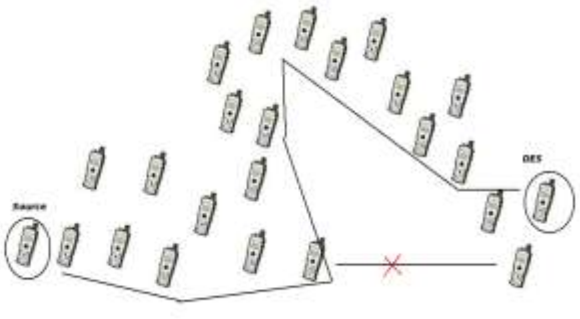

Fig.1 Ad-hoc network routing model

1) 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 using 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. In [7] paper author explains to reduce overhead problem in the proactive type routing protocols but not discussed about the overhead problem in the reactive type routing protocols. In [8] paper, author discusses the advantages and disadvantages of topology-based and position-based routing protocols and explores the motivation behind their design and trace the evolution of these routing protocols.

In [9] paper author summarizes the characteristics of representative routing protocols that have either been used or designed specifically for

MANET's and also indicated the type and subtypes whether they are topology-based or position-based and whether they are proactive/reactive, dtn or non-dtn, overlay or not. In [10] paper, author analyze a position-based routing approach that makes use of the navigational systems of vehicles and compare this approach with non-position-based ad-hoc routing strategies (dynamic source routing and ad-hoc on-demand distance vector routing). The first detailed micro-level analysis of pathologies for geographic face-based routing protocols, in the presence of location errors in static sensor networks was done but the location errors can severely degrade performance in location-based forwarding schemes, making accurate location information a necessity for most geographic routing protocols. Author presented a new metric for routing in multi-radio, multi-hop wireless networks. Author focused on wireless networks with stationary nodes, such as community wireless networks. The goal of the metric is to choose a high-throughput path between a source and a destination. Our metric assigns weights to individual links based on the expected transmission time (ett) of a packet over the link. The ett is a function of the loss rate and the bandwidth of the link. The individual link weights are combined into a path metric called weighted cumulative ett (wcett) that explicitly accounts for the interference among links that use the same channel. The wcett metric is incorporated into a routing protocol that author call multi-radio link-quality source routing. Wireless mesh networks (WMNS) have emerged as a key technology for next-generation wireless networking. Because of their advantages over other wireless networks, WMNS are undergoing rapid progress and inspiring numerous applications. However, many technical issues still exist in this field. In order to provide a better understanding of the research challenges of WMNS, this article presents a detailed investigation of current state-of-the-art protocols and algorithms for WMNS. Open research issues in all protocol layers are also discussed, with an objective to spark new research interests in this field. Location based routing is difficult when there are holes in the network topology and nodes are mobile. Terminal node routing, presented in this paper, addresses these issues. It uses a combination of location based routing (trr), used when the destination is far, and local routing(tlr), used when the destination is close. Trr uses anchored paths, a list of geographic points (not nodes) used as loose source routing information. By virtue of these characteristics, position-based routing protocols are highly scalable and particularly robust to frequent changes in the network topology. Furthermore, since the forwarding decision is made on the fly, each node always selects the optimal next hop based on the most current topology. But the route selection is based on the periodic update of location information

Inaccurate [11] local topology knowledge and the outdated destination position information can lead to inefficient geographic forwarding and even routing failure. Proactive local position distribution can hardly adapt to the traffic demand. It is also difficult to pre-set protocol parameters correctly to fit in different environments. We have developed two self-adaptive on-demand geographic routing schemes. The local topology is updated in a timely manner according to network dynamics and traffic demands. Our route optimization scheme adapts the routing path according to both topology changes and actual data traffic requirements.

II. Proposed solution:

We consider a MANET and define as communication neighbors of devices all the other devices that it can reach directly with its range. We assume that each device knows its own location and that it distributes a common time reference with the other devices: both needs can be met by equipping communication devices with GPS receivers. We propose a shared cooperative scheme for NPV, which enables a node, hereinafter called the verifier, to discover and verify the position of its communication neighbors and energy based attack solution.

III. **Modules**

We have divided our Enhanced technique into small modules for improving our implementation work: 1) Route discovery by Rreq, 2) Energy updating, 3) Calculating hop-by-hop energy, and 4) Route selection.

3.1.1) **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.

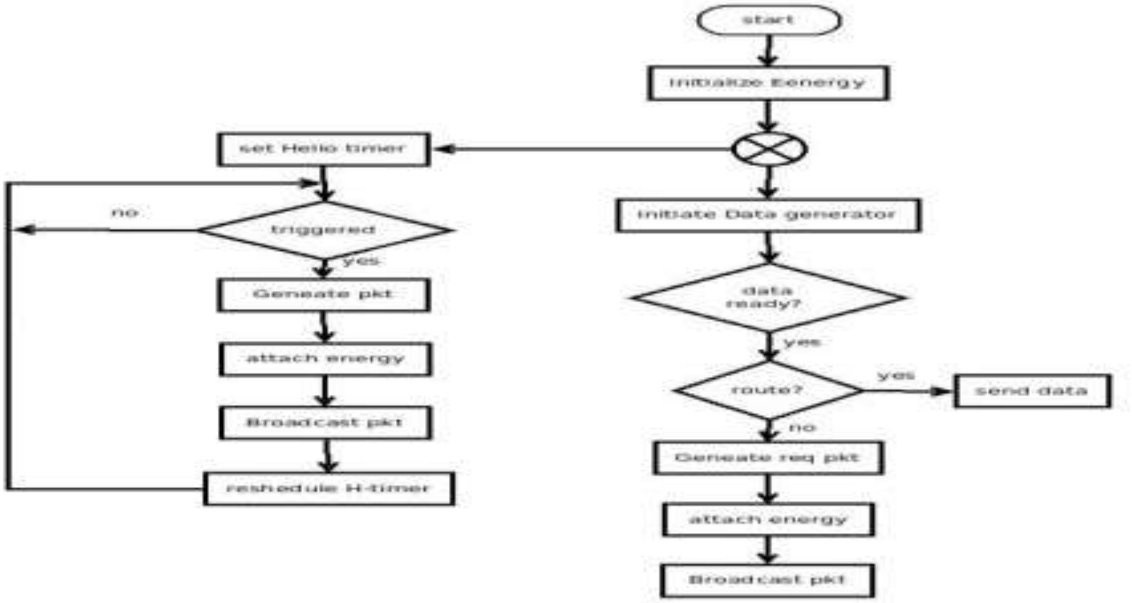

Fig.2 flow chart for energy efficient routing

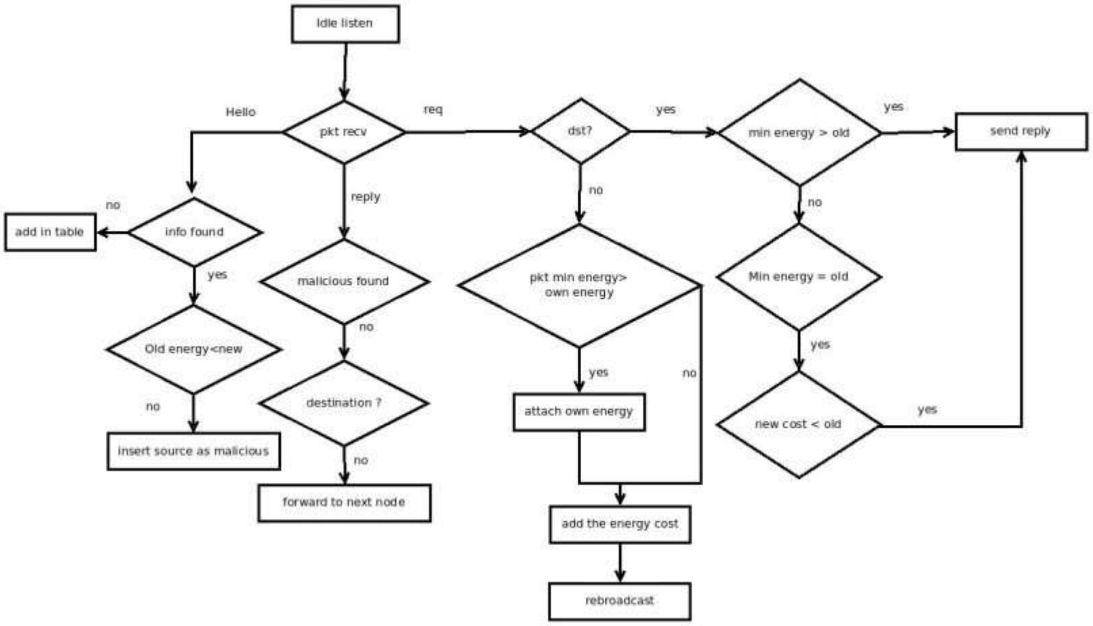

Fig.3 Flow chart for Energy based Attacker finding

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) **Route selection:**

Finally destination node receive the rreq and also it know the energy cost of both hop-by-hop also end-to-end communication. After validate these factors destination will send rrep through the high energy path.

3.5) **Algorithm:**

```
1) Set initial energy level for each node
2) Initialize hello timer
3) If hello timer triggered
     a. Generate the hello message
        i. Attach current energy
     b. Broadcast the pkt
4) If node has data
     a. If route is found
        i. Send data to next node
     b. Else
        i. Generate the req
           1. Attach energy level with pkt
        ii. Broadcast req
5) If node received packet
     a. If packet is hello packet
        i. Checks database
           1. If old energy is less than current energy
              a. Set as misbehavior node
     b. If packet is req
        i. If received node is destination
           1. Check in routing table
              a. If old min energy is less than new
                 i. Accept and send reply
              b. If old min energy is equal to new
                 i. Checks the energy cost
                    1. If old cost is more than new
           2. Ignore the packet
        ii. If node is intermediate node
```

```
            1. If pkt is duplicate or prev node is malicious
                a. Ignore pkt
            2. Else
                a. Check in routing table
                  i. Add the energy cost
                 ii. If pkt min energy is more than own
                        1. Add own energy as min energy
                iii. Forward the pkt
        c. If pkt is reply
            i. If prev node is malicious
                1. Ignore the packet
           ii. Else
                1. If node is not destination
                    a. Forward the pkt
```

Result Analysis:

We have simulated our proposed solution and enhanced solution with popular simulator such as ns2, and we got two types of results one is NAM and another one is Xgraph. The position finding and malicious node detection animation model is shown in fig.4 and 5

Fig.4 simple attack

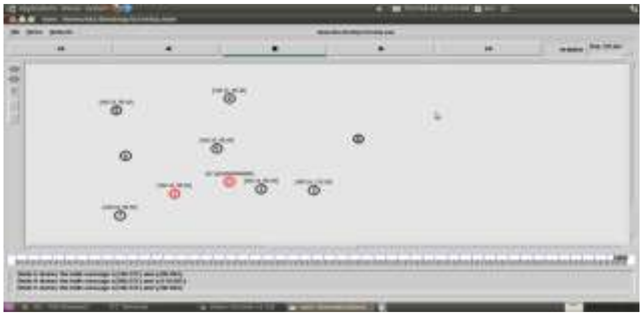

Fig.5 collusion attack

The figure 6 shows the false detection ratio. From our simulation we can get know false detection ratio increases while number of combined attacker get increase.

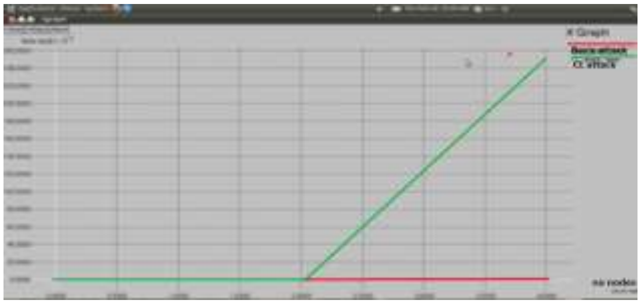

Fig.6 false detection

The figure 7 shows that the false detection ratio reduced when coverage area increase

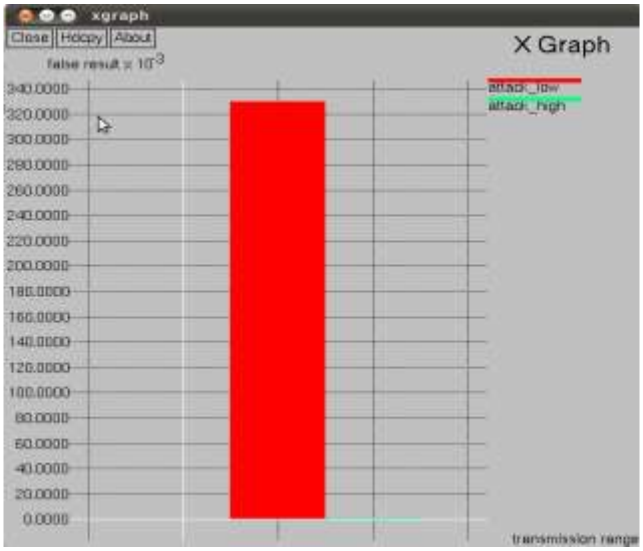

Fig.7 comparison of attack detection in low and high coverage area nodes

The figure 8 shows that our proposed solution effectively avoiding the attacker node and it selects the best path

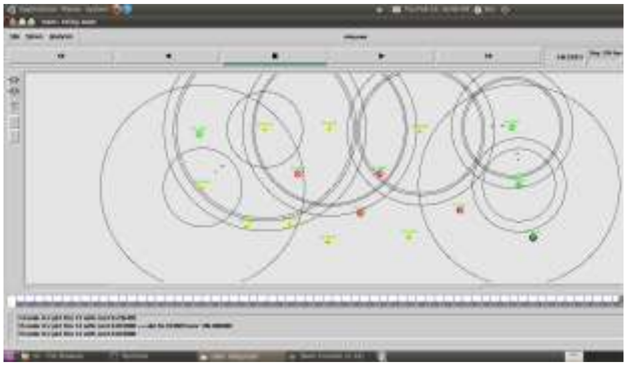

Fig.8 energy based attacker detection

Conclusion:

We successfully simulated our proposed solution for MANET. The development of ad hoc networking protocols and position-aware services require that mobile nodes learn the position of their neighbors. However, such a process can be easily abused or attacked by adversarial devices. In absence of a-priori legitimate nodes, the finding and checking of neighbor positions presents challenges that have been rarely investigated in the literature. We addressed this open issue by proposing a distributed coordinating solution that is strong against independent and group adversaries, and in our enhancement work we addressed the energy based adversary attack. . In future to improve the hacking detection, we will use position details by using GPS service

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

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.

7) *A routing strategy for mobile ad-hoc networ in city environments*---> christian lochert, hannes hartenstein, jing tian, holger füßler dagmar and hermann martin mauve.

8) Routing in multi-radio, multi-hop wireless mesh networks

9) A survey on wireless mesh networks: ----*ian f. Akyildiz, georgia institute of technology xudong wang, kiyon, inc.*

10) Distributed quality-of-service routing in ad hoc networks:------ shigang chen and klaranahrstedt, *member, ieee*

11) *“ad-hoc on-demand distance vector routing”,* charles e. Perkins, elizabeth m. Royer.

12) *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.

13) L. Blazevic, s. Giordano, and j.-y. Leboudec, “a location based routing method for mobile ad hoc networks”, mar. 2005.

14) Xiaojing xiang, zehua zhou, “self-adaptive on demand geographic routing protocols for mobile ad hoc networks”, 2007