



Self Protecting Nodes for Secured Data Transmission in Energy Efficient MANETs

Chandrakant N

Bangalore, Karnataka,
India

Abstract— This research article tries an novel approach to find out the solution for Energy and Security related issues in MANETs. This paper tries to evaluate two major properties of MANETs which are very crucial for Mobile Ad Hoc Networks to serve energy efficient and secured communication among nodes. In this network all nodes are distributed with unique identification number and its battery or energy level. All nodes in the network are having a protocol to acknowledge the data sensor nodes after certain interval. In the first scenario, if any unauthorised node(s) tries to access this network then victim node anyhow will receive a acknowledge packet with crucial credential which is understood by the victim node(s) only, using this data, the victim node will take a secured path to send the data other than attacking node. In the second scenario, when a victim node tries to find out a central or immediate neighbour, before sending its data, the victim node will try to find the energy level of each neighbour and energy required for each communication, based on these criteria, the victim node will choose the neighbour for communication. Hence this proposal would be great helpful to MANETs.

Keywords— Energy, Ad Hoc, Self Protection, WSN, Security

I. INTRODUCTION

Security is a primary concern in order to give protected communication between mobile nodes of MANETs. The attacks on MANETs will happen due its open mobile infrastructure in which nodes any node can join and leave easily with dynamics requests without a static path of routing. The various attacks can be done on layers of MANETs, application layer can be attacked by Malicious node, Repudiation; transport layer can be messed up by session hijacking, flooding; network layer can be attacked by Sybil, flooding, black hole, grey hole, worm hole, link spoofing, link withholding, location disclosure; data link/MAC layer can be attacked by malicious code, selfish behaviour; physical layer can be attached by interference, traffic jamming and eavesdropping. Power or energy is an extraordinary resource in MANET and it often affects the communication actions in network. So, we should be very careful in energy consumption. We need to see how each node can transmit its state between power save mode and active modes e.g. sleep/wake up mode. Ad hoc network imposes certain constraints on the communicating nodes, which broadly include the node mobility which results in a continuously changing network topology, limited bandwidth as it is wireless network, limited processing power due to its size and cost constraints. This paper simulates the secured communication and energy management algorithm for Ad Hoc networks.

II. RELATED WORK

Before starting this paper, it has below history as its input to motivate the research article. Paper [1] proposes a NCS system, which basically talks about integrating Mobile Computing and Cloud Computing to support wide heterogeneous applications via middleware services. The N-Care System offers many advantages over current systems. The use of cloud infrastructure increases the computational power of the system. In such a system, computation is done using the cloud infrastructure rather than by individual sensor nodes. As a result the power requirements and size of each sensor can be reduced. Smaller sensors are easier to sustain in times of an emergency such as a natural calamity and to conceal for detecting crime. Additionally, NCS offers a high degree of scalability. As a result it can handle increase in number of sensor nodes without much performance overheads. Since the system is dynamic, back-up sensors can be enabled, in case the main sensors fail. NCS can be utilized to collect data from different types of heterogeneous sensors and to provide domain specific sensor data to the end users. Paper [2] by Anfeng et al. proposed a technique to formulate the secret-sharing-based multipath routing problem as an optimization problem. The objective is to maximizing both network security and lifetime subject to the energy constraints [4][5][6][7][8]. As a summary, a three-phase disjoint routing scheme called the Security and Energy-efficient Disjoint Route (SEDR) was proposed. Based on the secret-sharing algorithm, the SEDR scheme depressively and randomly delivers shares all over the network in the first two phases and then transmits these shares to the sink node. Both theoretical and simulation results demonstrated that the proposed scheme has significant improvement in network security under both scenarios of single and multiple black holes without reducing the network lifetime.

Paper [3] by Praveena et al, has studied about symmetric key cryptography and public key cryptography and its own problems for Ad Hoc networks. In contrast to this prejudice, they proposed a method to increase the lifetime of a MANET/WSN by minimizing the energy cost of transporting information from a set of sources nodes to the sink nodes and for achieving security they have used a new public-key encryption technology called identity-based encryption (IBE) which allows to calculate a public key directly from a user's identity. By calculating public keys instead of generating them randomly, many of the difficulties that make encryption technology difficult to deploy and maintain are eliminated, making encrypted communications much easier to implement than in the past.

III. ALGORITHM AND RESULTS

In this section, the basic algorithm used for simulation and its results are going to discuss. Algorithm-1 shows the pseudo code of basic procedure, the MANETs network will have N number of nodes which are distributed with unique identification number and its power or energy level. All nodes in the network are having responsibility to acknowledge the data sensor nodes after certain interval. If any malicious node(s) tries to access this network/node then victim node will wait for acknowledge packet (anyhow it will receive a acknowledge packet in regular communication) with crucial credential which is understood by victim node(s) only, using this data, the victim node will evaluate and compare its usual data like keys, response time, path key, etc, then it will take a secured path to send the data other than attacking node, this is called as Self Protecting Node. With respect to energy consumption, when a victim node tries to find out a central or immediate neighbour after affecting by malicious attack, before sending its any data via alternative path, the victim node will find the energy level of each neighbour and energy required for each communication, based on the energy saving criteria, the victim node will choose the neighbour for communication.

Algorithm-1: Secured Communication with Energy Efficiency

```
1: N=>Number Of Nodes, i=>Source Node, A[]=>Nodes List ,k=>Destination/Neighbour Node
2: for i=0,i<N,i++
3: A[i]=>Sends Data to A[k]
4: if A[k] is Malicious, then wait for ACK and failed in validation
5: if BatteryLevel of A[k+1] != Satisfactory then choose other neighbour
6:else use A[k+1]
7:end if
8: else continue communication
9: end if
10: end for
```

Fig 1 shows the example of communication among nodes in the network. This network has nodes like A, B, C, D and E with power level 40,50,20,80 and 90 percent respectively. Here B,C,D are neighbours to A. Say node A is a source and E is a destination, B is a malicious node and responded to node A while A tries to reach E, now A will expect an acknowledgement from node E but receives B's acknowledgement, A will try to evaluate this packet w.r.t keys, response time, node details etc. This packet is not genuine since B is a fraud intention node. Now A has left with two neighbours C and D. So, it has to choose any one of them. Energy level of C and D has 20 and 80 percent respectively. Since C node is having lower energy level and it will be exhausted if it is used for communication, hence choosing D node makes more sense for intermediate communication agent considering energy level.

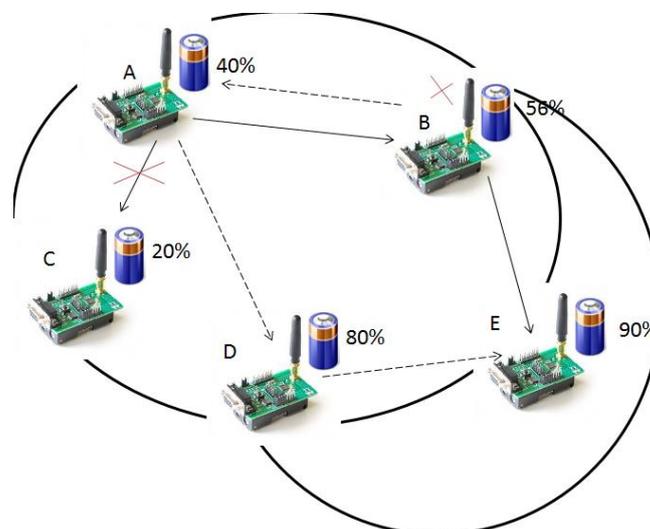


Fig. 1 MANET's Communication Model

Fig 2 shows the energy consumption of 50 nodes with 10J energy for each node, comparing with OLSR (Optimized Link State Routing), the proposed algorithm is showing better results w.r.t energy saving.

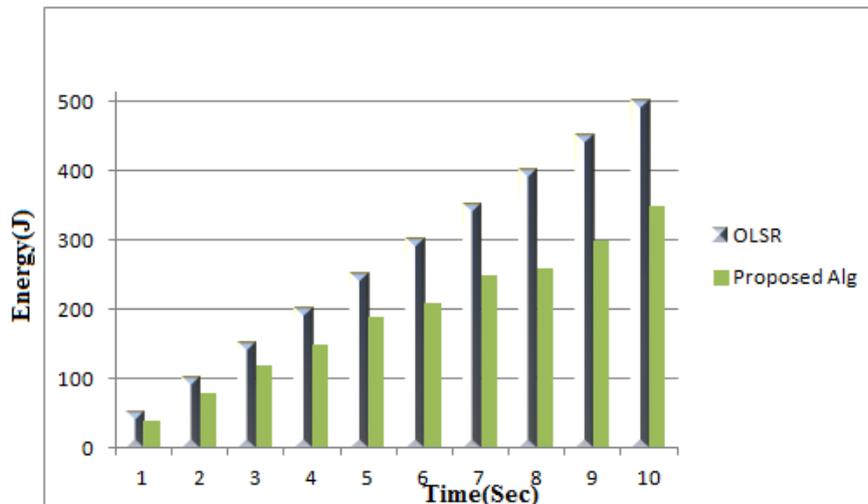


Fig. 2 Energy Consumption of 50 Nodes

IV. CONCLUSIONS

A novel approach of securing data with energy constraints has been simulated and presented in this paper. In this network when a victim node tries to find out a central or immediate neighbour for communication, before sending its data, it will find the energy level of each neighbour and energy required for each communication, considering these things, victim node will choose the neighbour for communication. Hence this proposal would be a one of the great solution for resource constraints with security. The upcoming and future network should be aware of all its resource and security constrains.

REFERENCES

- [1] Chandrakant N, Bijil A P, Puneeth P, Deepa Shenoy P, Venugopal K R, L M Patnaik, "WSN Integrated Cloud Computing for N-Care System(NCS) Using Middleware Services", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278 - 3075, Volume - 3 , Issue - 1, June 2013.
- [2] Anfeng Liu, Zhongming Zheng, Chao Zhang, Zhigang Chen, Xuemin Shen, "Secure and Energy-Efficient Disjoint Multipath Routing for WSNs", IEEE Transactions on Vehicular Technology (Volume:61, Issue: 7), pp 3255 - 3265 Sept 2012 .
- [3] Praveena A, Devasena S, Chelvan KMA, "Achieving energy efficient and secure communication in wireless sensor networks", IFIP International Conference on Wireless and Optical Communications Networks, pp 1 - 5, 2006.
- [4] Christina, Melmaruvathur, "Energy efficient secure routing in wireless sensor networks", International Conference on Emerging Trends in Electrical and Computer Technology (ICETECT), pp 982 - 986 , 2011.
- [5] Sang-Eon Lee, Daegu, Sang-Ho Shin, Geum Dal Park, Kee-Young Yoo, "Wireless Sensor Network Protocols for Secure and Energy-Efficient Data Transmission", Computer Information Systems and Industrial Management Applications, pp 157-162, 2008.
- [6] Sen J, "Secure and energy-efficient data aggregation in Wireless Sensor Networks", 2nd National Conference on Computational Intelligence and Signal Processing (CISP), pp 23, 2012.
- [7] M. Kim , E. Jeong , Y. C. Bang , S. Hwang and B. Kim "Multipath energy-aware routing protocol in wireless sensor networks", Proc. IEEE INSS, pp.127 -130, 2008.
- [8] Y. Challal , A. Ouadjaout , N. Lasla , M. Bagaa and A. Hadjidj "Secure and efficient disjoint multipath construction for fault tolerant routing in wireless sensor networks", J. Netw. Comput. Appl., vol. 34, no. 4, pp.1380 -1397, 2011.