Secure and Reliable Routing using PSO optimization

Amali Angel Punitha, S.Anu Priya, P.Tharani and S.Priyadharshini

Ultra college of engineering and technology for women

Abstract: *Wireless sensor networks (WSNs) are increasingly being deployed in security-critical applications . To conquer that challenge, an active detection-based security and trust routing scheme named Active Trust is proposed for WSNs The most important innovation of Active Trust is that it avoids black holes through the active creation of a number of detection routes to quickly detect and obtain nodal trust and thus improve the data route security . PSO optimization has been used to choose a best routing path. NS2 Simulation results demonstrate that our routing protocols can improve the packet delivery ratio and route stability*

Introduction

Mobile means 'moving' and ad-hoc means 'temporary without any infrastructure'. Therefore, a mobile ad-hoc network is made up of group of mobile nodes, which cooperates to communicate with each other without any fixed central base station . A mobile ad hoc network (MANET), sometimes called a mesh mobile network, is a network of mobile devices connected by wireless links. MANET is a kind of point to point transmission type and is a group of mobile nodes communicating with each other by wireless [14]. Due to infrastructure-less nature of the network, routing and network management is done cooperatively by the nodes i.e. the nodes themselves maintains the functioning of the network . The topology of the network varies rapidly and unpredictable over time because of the mobility of the nodes. Besides, the security of MANET has many defects. These threats make the security of MANET lesser than a cable network and produce many security issues. Because the communication of MANET uses the open medium, attacker can easily overhear message that are transmitted. The design of previous routing protocol trusts completely that all nodes would transmit route request or data packets correctly, dynamic topology, without any central infrastructure, and lack of certification authorities make MANET vulnerable to diverse types of attacks . One of common attack is Black hole attack that is a malicious node can attract all packets by using forged RREP to falsely claiming a fresh and shortest route to the destination and then discard them without forwarding them to the destination . Black hole attack is a kind of Denial-of-Service attacks and derive Gray hole attack, a variant of black hole that selectively discards and forwards data packets when packets go through it . Cooperative black hole attacks mean several malicious nodes cooperate with each other and work just like a group. This kind of attack results in many detecting methods fail and causes more immense harm to all network .

Trust is one’s degree of belief about the future behavior of another entity (node). It is based on the one’s past experience with and observation of the other’s actions. Trust management involves formulating evaluation rules and policies, representing trust evidence, and evaluating and managing trust relationships. It was first introduced as a separate component of security in network services and given an overall definition in [2]. After that, considerable research on the topic follows. Thus far, many trust management systems have been introduced in literature. They can be divided into two main categories: *credential-based* and *reputation-based*. In most credentialbased systems, the trust relation between nodes is established by managing and exchanging credentials which should be verified and restricted by a preset policy. These systems usually make a binary decision, whether to trust or distrust a node. Because of this binary approach, they lack flexibility. On the other hand, reputation-based systems perform better by focusing on the evaluation of trust value. They calculate the trust value of a node by gathering observations of the node’s behavior in the past. A trusted node is one that always normally complete their assigned tasks; an untrustworthy node is one that does not provide desired services or provide abnormal services .

BACKGROUND AND RELATED WORK

In this section, we introduce the basic concepts in anonymous routing, and provide a short survey on the existing routing protocols.

A. Anonymity and Security Primitives

We introduce some common mechanisms that are widely used in anonymous secure routing.

1) Trapdoor: In cryptographic functions, a trapdoor is a common concept that defines a one-way function between two sets A global trapdoor is an information collection mechanism in which intermediate nodes may add information elements, such as node IDs, into the trapdoor. Only certain nodes, such as the source and destination nodes can unlock and retrieve the elements using pre-established secret keys. The usage of trapdoor requires an anonymous end-to-end key agreement between the source and destination.

2) Onion Routing: It is a mechanism to provide private communications over a public network . The source node sets up the core of an onion with a specific route message. During a route request phase, each forwarding node adds an encrypted layer to the route request message. The source and destination nodes do not necessarily know the ID of a forwarding node. The destination node receives the onion and delivers it along the route back to the source. The intermediate node can verify its role by decrypting and deleting the outer layer of the onion. Eventually an anonymous route can be established.

3) Group Signature: Group signature scheme can provide authentications without disturbing the anonymity. Every member in a group may have a pair of group public and private keys issued by the group trust authority (i.e., group manager). The member can generate its own signature by its own private key, and such signature can be verified by other members in the group without revealing the signer's identity. Only the group trust authority can trace the signer's identity and revoke the group keys.

B. Anonymous On-demand Routing Protocols

There are many anonymous on-demand routing protocols. Similar to the ad hoc routing, there are two categories: topology-based and location-based [1], or in other words, node identity centric and location centric . We compare the protocols in Table I, in terms of the key distribution assumption, node anonymity in route discovery, and packet authentication. Our observations are summarized as follows:

First of all, the routing protocols are designed to work in different scenarios. AO2P, PRISM, and ALERT are designed for location-based or location-aided anonymous communications, which require localization services. Since ours is for general MANETs, we focus on the topology-based routing rather than location-based routing. Secondly, as mentioned in Section I, SDAR, AnonDSR, MASK, and D-ANODR have problems in meeting the unindentifiability and unlinkability. The node IDs in a neighborhood and along a route are possibly exposed in SDAR and AnonDSR, respectively. The plain node IDs are used in the route request of MASK and D-ANODR

PROPOSED SYSTEM

Theory of particle swarm optimization (PSO) has been growing rapidly. PSO has been used by many applications of several problems. The algorithm of PSO emulates from behavior of animals societies that don't have any leader in their group or swarm, such as bird flocking and fish schooling. Typically, a flock of animals that have no leaders will find food by random, follow one of the members of the group that has the closest position with a food source (potential solution). The flocks achieve their best condition simultaneously through communication among members who already have a better situation. Animal which has a better condition will inform it to its flocks and the others will move simultaneously to that place. This would happen repeatedly until the best conditions or a food source discovered. The process of PSO algorithm in finding optimal values follows the work of this animal society. Particle swarm optimization consists of a swarm of particles, where particle represent a potential solution

VARIANT OF PSO

Exploration is the ability of a search algorithm to explore different region of the search space in order to locate a good optimum. Exploitation, on the other hand, is the ability to concentrate the search around a promising area in order to refine a candidate solution[3].With their exploration and exploitation, the particle of the swarm fly through hyperspace and have two essential reasoning capabilities: their memory of their own best position - *local best (lb)* and knowledge of the global or their neighborhood's best - *global best (gb).* Position of the particle is influenced by velocity. Let x(t) denote the position of particle in the search space at time step t ; unless otherwise stated, t denotes discrete time steps. The position of the particle is changed by adding a velocity, to the current position

$x(t+1)=x(t)+v(t+1)$

acceleration coefficient c1 and c2 and random vector r1 and r2 . Simple example of PSO, there is a function

min f(x)

where $x(b)<x<x(a)$

x(b) lower limit and x(a) upper limit

Assume that the size of the group of particle is N. It is necessary that the size N is not too large, but also not too small, so that there are many possible positions toward the best solution or optimal *Second*, generate initial population x with range x(b) and x(a) by random order to get the x1,x2…..xn . It is necessary if the overall value of the particle is uniformly in the search area Then calculate the speed of all particles. All particles move towards the optimal point with a velocity. Initially all of the particle velocity is assumed to be zero. Set iteration i=1 At the iteration, find the two important parameters for each particle j that is: The best value of xj(i) (the coordinates of particle j at iteration) and declare as $p_{best}(j)$, with the lowest value of objective function (minimization case) f[x{j}], which found a particle at all previous iteration. The best value for all particles xj(i) which found up to the i th iteration, Gbest with the value function the smallest goal / minimum among all particles for all the previous iterations, Calculate the velocity of particle *j* at iteration *i* using the following formula using formula (2): Where c1 and c2 , respectively, are learning rates for individual ability (cognitive) and social influence (group), r1 and r2 and uniformly random numbers are distributed in the interval 0 and 1. So the parameters c1 and c2 represent weight of memory (position) of a particle towards memory (position) of the groups (swarm). The value of c1 and c2 is usually 2, so multiply c1r1 and c2r2 ensure that the particles will approach the target about half of the difference Calculate the position or coordinates of particle j at the i th iteration by :

xi(t+1)=xi(t)+vi(t+1)

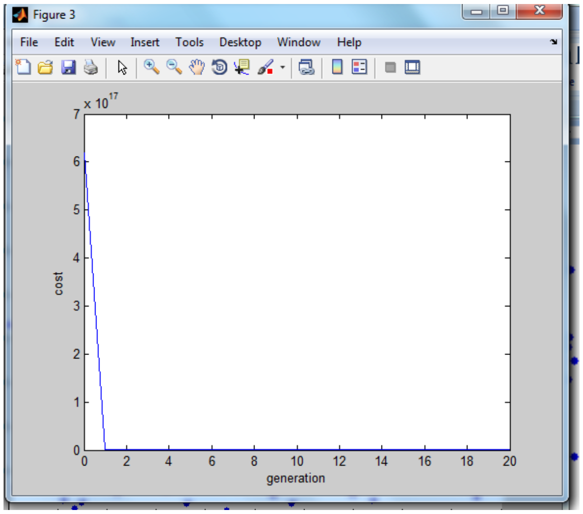
This iteration process continues until all particles convergence the same solution. Usually be determined by the termination criteria (Stopping criterion), for example the amount of the excess solution with a solution now previously been very small.

5.3.1 Constrained using PSO Algorithm

The following steps are used by the PSO technique to solve the unit commitment Problem

Step 1: Initialize a population of particles pi and other variables. Each particle is usually generated randomly with in allowable range.

Step 2: Initialize the parameters such as the size of population, initial and final inertia weight, random velocity of particle, acceleration constant, the max generation, Lagrange's multiplier (λi), etc.



Step 3: Calculate the fitness of each individual in the population using the fitness function or cost function.

Step 4: Compare each individual's fitness value with its pbest. The best fitness value among pbest is denoted as gbest.

Step 5: If the evaluation value of each individual is better than the previous ppbest, the current value is set to be ppbest. If the best ppbest is better than pgbest the value is set to be pgbest.

Step 6: Modify the λ and α for each equality and Inequality constraint

Step 7: Minimize the fitness function using PSO method for the number of units running at that time.

Step 8: If the number of iteration reaches the maximum then go to step 9. Otherwise go to step 3.

Step 9: The individual that generates the latest is the optimal generation power of each unit with the minimum total generation cost.

RESULTS AND DISCUSSIONS

For simulation, we are using MATLAB tool which mainly used in wireless sensor networks . hundred nodes created with sink node and PSO fiteness applied to twenty iteration of random population size

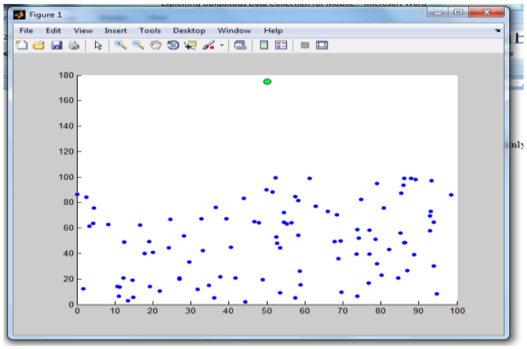


Fig node creation

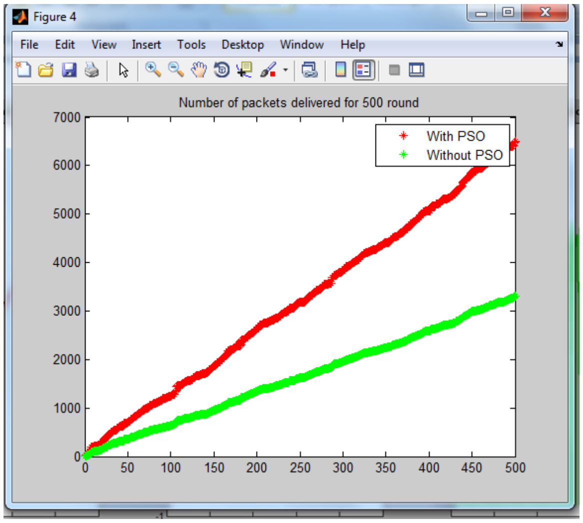
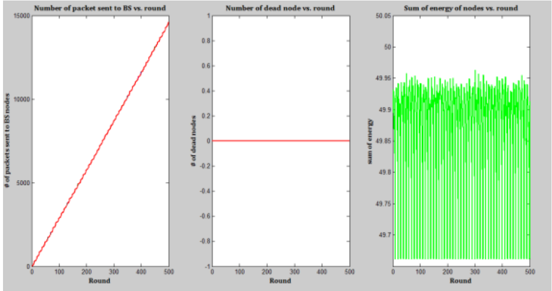


Fig population generation

Fig Energy reduction

Fig increased throughput ratio



Conclusion

Solving an optimization problem is one of the common scenario that occur in most engineering applications. Classical techniques such as LP and NLP are efficient approaches that can be used in special cases. In this project, considered the problem of finding optimal mobile data gathering strategies for energy harvesting sensor networks. scheduling and routing based on the individual energy harvesting rate such that the overall network utility can be maximized. Finally, we provided extensive numerical results under different scenarios to validate the efficiency of the proposed scheme and complement our theoretical analysis.PSO based approach reduces power consumption and reduce number of dead nodes in a routing path

References

[1] European Railway Agency. (2009). *Impact Assessment on the Use of Derailment Detection Devices in the EU Railway System, ERA/REP/03-2009/SAF*, accessed on Feb. 2, 2016. [Online]. Available: http://www.era.europa.eu/Document-Register/Pages/final-report-on-derailment-detection-device.aspx

[2] Knorr Bremse. *EDT101 Derailment Detection System*, accessed on Feb. 2, 2016. [Online]. Available: http://www.knorrbremse.de/en/ railvehicles/products/trainsafety/edt101.jsp

[3] *Recommendation Requiring the Use of Derailment Detection Devices,Text Provisionally Adopted During the 44th Session of the RID 2007 Committee of Experts Meeting in Zagreb*, RID Committee of Experts, Zagreb, Croatia, 2007.

[4] A. V. Vostroukhov, A. V. Metrikine, A. C. W. M. Vrouwenvelder, V. I. Merkulov, V. N. Misevich, and G. A. Utkin, "Remote detection of derailment of a wagon of a freight train: Theory and experiment," *Arch. Appl. Mech.*, vol. 73, pp. 75–88, Aug. 2003.

[5] M. Macucci, S. Di Pascoli, P. Marconcini, and B. Tellini, "Wireless sensor network for derailment detection in freight trains powered from vibrations," in *Proc. IEEE Int. Workshop Meas. Netw. (M&N)*, Coimbra, Portugal, Oct. 2015, pp. 1–6, doi: 10.1109/IWMN.2015.7322970.

[6] M. Kato and K. Terada, "Development of an evolution type train protection system to prevent secondary accidents," in *Proc. Int. Rail Safety Conf.*, Dublin, Ireland, 2006, pp. 1–10.