http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 9 (3): 506-511, 2010
ISSN 1812-5638

A Security Routing Optimization Scheme for Multi-hop Wireless Networks

Du Jun and Li Wei-Hua
School of Computer Science, Northwestern Polytechincal University, Xi'an 710072, China

Abstract: Selfish nodes and malicious nodes in large-scale ad hoc networks lead to poor performance and even paralyze the network. How to dismiss these nodes from routing table is important to improve the network security. In this study, a security aware routing optimization algorithm named SARO is proposed to achieve this. The SARO is an improvement to ant optimization. It utilizes reputations from a reputation system to derive the pheromone trail refresh process and visible functions. Abnormal nodes are discarded from routing tables and packets are routed along paths with least abnormal nodes. The SARO is a security enhancement to routing protocols, which can both improve security of network and enhance the network performance.

Key words: Multi-hop wireless network, routing protocol, ant colony algorithm, security

INTRODUCTION

An ad hoc network is formed by a set of nodes without any pre-deployed infrastructure. Since, no base stations are required, the most attractive advantage of ad hoc networks is that it can be deployed rapidly. It is applicable for temporary communication environments such as temporary conference and natural disaster rescue where, pre-deployment of network infrastructure is difficult or impossible (Gerla, 2004).

Security and efficiency are two basic requirements of these applications. However, in a large-scale wireless ad hoc network, some nodes may deny to forward packets from their neighbors to reserve limited power supply, which results in selfish node problem (Paul and Westhoff, 2002). In applications such as the battlefield communication and natural disaster rescue, it is possible that the enemy may deploy malicious nodes to attack the network. These nodes may attack the network at any layers of the network protocols (Gupta *et al*., 2002). And in another situation, constrained by limited radio spectrum, different networks may share the same frequency band, which results in mutual interference at the physical layer (Peha, 2000). These problems will lead to degradation of network performance and even paralyze the network. How to solve these problems is a challenging research issue of ad hoc network security.

In this study, an ant colony based routing optimization algorithm named SARO (Security Aware Routing Optimization) is presented. The SARO can optimize existing routing protocols for security. Most current ant colony optimization algorithms for wireless ad hoc networks are designed for shortest path or best link quality optimization (Gunes *et al*., 2002). However, the scheme proposed in this study is mainly focused on security enhancement. Optimized by SARO algorithm, nodes in the network avoid deliver packets to neighbors that are selfish or malicious, which can prevent the network from attacking and improve the security of ad hoc network dramatically.

AntHocNet (Di Caro *et al*., 2004) is the first ant colony based optimization scheme for ad hoc, which is an optimization to AODV. In this scheme, nodes in the network construct routing information according to AODV protocol. During delivering packets, nodes in the network send some probe packets (named artificial ant) to optimize routing information. Higher quality routing paths are selected for routing and paths with low quality are deleted from routing tables. In AntHocNet scheme, link quality is the only criteria used for optimization, security is not considered.

ARAMA (Hussein and Saadawi, 2003) is another ant colony algorithm for routing optimization. As nodes in ad hoc networks are limited by power resource, energy efficiency is very important to such networks. ARAMA scheme uses energy efficiency as criteria for optimization. Reference (Günes and Spaniol, 2003) suggested that ant colony optimization can be used for routing optimization, but which criteria can be used and how these criteria are used are not discussed.

Banerjee *et al*. (2005) proposed an ant colony optimization algorithm for security. The main purpose of this study is to detect attacks. Therefore, it is a distributed intrusion detection system. And further, this scheme changes most aspects of ant colony algorithms, which needs further theory validation.

This study proposes a novel ant colony based optimization algorithm, which is based on classical ACO.

Corresponding Author: Du Jun, School of Computer Science, Northwestern Polytechnical University, Xi'an 710072, China

The pheromone trail update methods and visibility function are adopted according to time variety character of wireless networks. Selfish nodes and malicious nodes are isolated from the network, which can improve the security of network dramatically.

SYSTEM MODEL

An ad hoc network can be denoted by a graph G = {V, E}, where, V is the set of nodes in the network and E is the set of connections in the network. Supposing the maximize communication distance for wireless devices between nodes is d, $e \in E$ means that $e = (v_m, v_n)$, $v_m \in V$, $v_n \in V$, $m \neq n$ and

$$\sqrt{(x_m - x_n)^2 + (y_m - y_n)^2} \leq d$$

In a large-scale ad hoc network, there are hundreds or thousands of nodes in the network. Some nodes may be temporarily disabled or destroyed. And the communication channel between nodes may be interfered by noise. Therefore, elements in E and V are all time variable.

First, we define two measure functions.

QoS function: $Q(e): Q \rightarrow C^+$, which defines QoS parameters for connection e including transmission delay, bandwidth, delay jitter and packets loss rate.

Trust function: $T(e): T \rightarrow C^+$, which defines trust degree of neighbor on the other hand of link e. T(e) is usually calculated using a trust model. As described in (Buchegger and Le Boudee, 2005) a trust model is usually implemented by a Bayesians process based on captured packets of neighbors.

As E and V are time variable, V(e) and T(e) are time variable too.

BASIC ACO PROCESS

Ant colony algorithm is inspired by the actions of ants when they are looking for food. It is mainly used for routing optimization in graphs. It is the most practical swarm intelligence algorithm (Kennedy and Eberhart, 2001), which is already used in machine learning and bioinformatics, as well as the areas of wired network routing optimization.

For example, in the application of wired network routing optimization, nodes in the network send some probe packets first. These packets are routed to the destination and are used for optimization purpose. These packets drop pheromone trail on their way to the destinations. Those nodes with higher rank receive more pheromone trail. These probe packets are delivered by the sender to its neighbors with the probability calculated by pheromone trail. The more pheromone trail the link has, the higher probability the packets delivered. After several iterations, nodes with higher pheromone trail are selected for packets routing.

Before description of the algorithm, we first give some definitions.

Definition 1: Probabilistic Rule.

Supposing that ant k is currently received by node v_i and there are several neighbors can be selected as next hop to its destination, the probability that node v_j is selected as next hop is:

$$P_{ij}^k(t) = \begin{cases} \dfrac{(\tau_{ij})^{\alpha}(\eta_{ij})^{\beta}}{\sum_{l \in N_i^k}(\tau_{il})^{\alpha}(\eta_{il})^{\beta}}, & \text{if } j \in N_i^k \\ 0, & \text{otherwise} \end{cases} \quad (1)$$

where, P_{ij}^k is the probability that node v_i select connection $e(v_i,v_j)$ as next hop and τ_{ij} denotes the amount of pheromone trail on connection $e(v_i,v_j)$. η_{ij} denotes the visibility function of node v_j. α, β are parameters that control the relative importance of trial versus visibility.

Definition 2: Pheromone trails update rule.

After ant k reaches its destinations, the path length is l, we define the pheromone trails update rule as:

$$\tau_{ij}(t+l) = \rho\tau_{ij}(t) + \Delta\tau_{ij}(t, t+l) \quad (2)$$

$$\Delta\tau_{ij}(t, t+l) = \sum_{k \in R}\Delta\tau_{ij}^k(t, t+l) \quad (3)$$

where, $\Delta\tau_{ij}$ (t, t+*l*) is increment of pheromone trails for connection(v_i, v_j), ρ is a coefficient ($0<\rho<1$) such as $1-\rho$ represents evaporation of pheromone trails. $\Delta\tau_{ij}^k$ (t, t+1) is the increment of pheromone trails for connection (v_i, v_j) during (t, t+l) left by ant k.

After these definitions we give a brief description of ACO optimization algorithm:

- **Step 1:** At regular intervals, from every network node, a forward ant k is launched with the mission to find a path until the destination. The identifier of every visited node is saved onto a memory Vlists and carried by the ant
- **Step 2:** At each node v_i, a forward ant selects the next hop node v_j using the probability mentioned in Eq. 1

In Eq. 1, if α is greater than β, the pheromone trails are more important than visibility function. Otherwise, visibility function is more important than pheromone trails.

- **Step 3:** When forward ant k reaches its destination, it is transformed into a backward ant k' whose mission is to update the pheromone trail of the path it used to reach the destination and which is stored in its memory
- **Step 4:** Before the backward ant k starts its return journey, the destination node computes the amount of pheromone trail $\Delta\tau_{ij}$ (t, t+1) that the ant can drop during its journey. The better security parameters, the higher pheromone trails
- **Step 5:** Whenever a node v_i receives a backward ant k' from a neighboring node v_j, it updates its routing table in the manner mentioned in Eq. 2 and 3
- **Step 6:** When the backward ant k' returns to the source node, its mission is finished and the ant is dropped

SECURITY AWARED ROUTING OPTIMIZATION (SARO)

The algorithm descript in above section is the classical procedure of ACO. It does not take characters of wireless network and security into considerations. In this section we will describe enhancements to classical ACO considering characters of both wireless network security. The main enhancement includes pheromone trails update rule, probabilistic rule and pheromone trails update time. Detailed description is presented in the following subsections.

Process of selfish nodes and malicious nodes: The approaches available do not make a difference on dealing with selfish nodes and malicious nodes. However, it is easy to conclude that selfish node is less harmful than malicious nodes. The selfish node just discards packets from neighboring nodes. But malicious node may attack the network by generate faked packets. Malicious node may lead their neighboring nodes to abnormal state. While selfish nodes does not affect its neighboring nodes. Therefore, these two types of nodes should be processed differently. To the best of our knowledge, this is the first attempt on security routing optimization of ad hoc networks.

if node v_i is declared to be a selfish node by the reputation system then

Reputation of its neighboring node v_n is T_n;

else if node v_i is declared to be a malicious node by the reputation system then

reputation of its neighboring node v_n should be $T_n = \min\{ T_n, T_i \}$

endif

The reputation system can be adopted from P2P reputation systems that are widely used (Buchegger and Le Boudee, 2005). By using the process mentioned above, malicious nodes and their neighboring nodes are all deleted from routing tables. This is reasonable because neighboring nodes of malicious nodes may act abnormally as malicious nodes may attack these nodes.

Time sensitivity enhancement for ACO: Different from wired network, the channel status of wireless device are time variable. Most wireless parameters such as bandwidth, network bandwidth are also time variable. But the pheromone trails update process is not time sensitive. Therefore, our second novel enhancement is time sensitive enhancement to pheromone trails evaporation process.

We add a timer to the nodes of the network. On time out, the pheromone trails evaporation process is carried out, which is a modification to Eq. 2 and 3.

ON timer:

$$\tau_{ij} = \rho\tau_{ij} \tag{4}$$

ON Optimization:

$$\tau_{ij}(t+1) = \tau_{ij}(t) + \Delta\tau_{ij}(t, t+1) \tag{5}$$

By such modification, the pheromone trails evaporation process is time sensitive, which is more suitable for time variable wireless ad hoc networks.

Definitions for SARO: First, as to the construction of visibility function, we define η_{ij} as following:

$$\eta_{ij} = (T_e)^{\sigma_A} \times (Q_e)^{\sigma_B} \tag{6}$$

where, Q_e, T_e are QoS function and trust function for connection $e(v_i, y_j)$, respectively. While σ_A, σ_B are parameters controlling the importance of QoS versus security.

As QoS parameters and security parameters are considered in visibility function, three parameters are used in selecting the next hop in Eq. 1, which are QoS, trust and cumulated pheromone trails. Connections with higher quality, more security and more pheromone trails are more likely to be selected as next hop.

Second, by considering trust parameter of nodes, we define pheromone trail update rule as following:

$$\Delta\tau_{ij}^{k}=\left(\frac{1}{d_k}\right)^{\mu_A}\times\left(\prod_{i,j\in VLists}T_e(i,j)\right)^{\mu_B}\times\left(\prod_{i,j\in VLists}Q_e(i,j)\right)^{\mu_C} \quad (7)$$

where,

$$\prod_{i,j\in VLists}T_e(i,j)$$

is the product of trust parameters collected by ant k on its way to its destination.

$$\prod_{i,j\in VLists}Q_e(i,j)$$

is the product of QoS parameters collected by ant k on its way to destination.

Description of SARO: We give two data structures that are used in our SARO (Security Aware Routing Optimization) algorithm.

First, we define the routing table structure named SARO-T for nodes in the network. SARO-T appends several fields to current routing tables.

As a example, routing table in node v_i includes entries pointing to it neighboring nodes, which is shown in Fig. 1. Supposing that node v_n is one of its neighboring nodes.

- Dest: Address of the destination
- Next Hop: Address of the next hop that can route packets to Dest
- Pher: Accumulated pheromone trails τ_{iu} on connection e_{iu}
- QoS: QoS parameter $Q_e(i,u)$ for connection e_{iu}
- Trust: Trust parameter $T_e(i,u)$ for node V_n

Second, we define data structure of artificial ant SARO-ANT. According to principle of ACO, ant must carry information of all nodes it passed.

In our security aware ACO, the structure of SARO-ANT includes the following fields (Fig. 2).

Dest	Next Hop	Pher	QoS	Trust

Fig. 1: Structure of SARO-T

Id	Scr	Dest	VLists	TTL

Fig. 2: Data Structure of SARO-ANT

- Id: Sequence number of artificial ant
- Src: Source address of artificial ants
- Dest: Destination address of artificial ant
- Vlists: Vectors of all nodes that the ant visited
- TTL: Maximal life of the ant

And further, the structure in Vlists can be expressed as <Addr, QoS, Trust>.

Algorithm 1: SAROOPT
Input: Reuest (sourceID, destinationID).
Output: Optimized routing information: SARO-T.
Initialization: t = 0; Timerout = T

- Step1: Node v_S wants to optimize its routing to destination and sends m probe packets with a certain interval. Its next hop node forwards this packet to its next hop with probability $P_{v_S\mu}^{k}(t)$
  SARO-ANT.TTL = 0
  if forwarded then
  SARO-ANT.TTL++;
  if SARO-ANT.TTL>T then
  Drop this probe packet;

- **Step 2:** When packet k(k≤m) arrives node v'
  if v' ≠ destinationID
  if v' ∈ VLists
  Delete first v' from VLists and forward packet k with $P_{v'\mu}^{k}$
  else forward probe packet k with probability $P_{v'\mu}^{k}$
  else go to step 3

- **Step 3:** if = destinationID
  Calculate the return path l'_k to source address using l_k in VLists and calculate increment of pheromone trails $\tau_{v_iv_j}$ (t) according to Eq. 7. Construct backward probe packet k' and deliver it to v_S.

- **Step 4:** During the returning journey of k', all nodes in the path update its own pheromone trails τ_{ij} according to Eq. 5 and update the information in SARO-T accordingly
- **Step 5:** Having received all response of m probe packets or the timeout time is reached, the source nodes return to normal status and the optimization is finished

As mentioned earlier, the pheromone trails are evaporated every T_n according to Eq. 4.

SIMULATION RESULTS

We implement SARO in NS-2 simulator. In our experiments, no mobility of nodes is simulated. Static

Table 1: Simulation environment configurations (ns-2.34)

Terrain-dimensions	2000M×2000M
Mobility	None
Prop-pathloss	Two-ray
Noise-figure	10.0
Temperature	290.0K
Radio-type	Radio-accnoise
Radio-frequency	2.4 GHz
Radio-bandwidth	2 MBPS
Radio-rx-type	BER
Radio-tx-power	15.0 DBm
Routing-protocol	Static

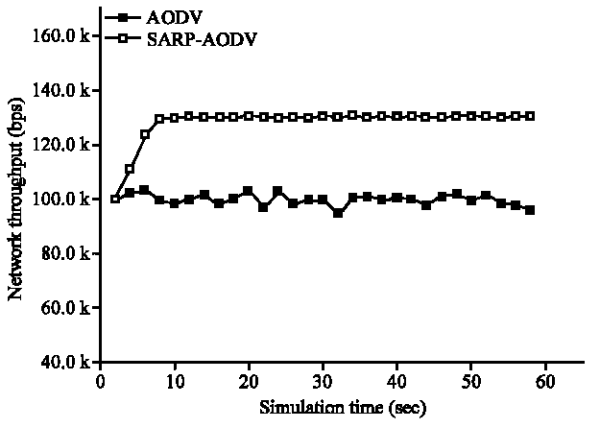

Fig. 3: Throughput of the network

routes are pre-configured; no routing protocol is used. Please refer to Table 1 for detailed simulation parameters.

First, to evaluate the security enhancement for routing protocols, we implements a security optimized routing protocol named SARO-AODV, which combines SARO and AODV protocols. And we compare its security performance with traditional AODV protocol. In this simulation, the network is composed of 100 nodes, with topology of 10 X 10 grid topology. Three nodes are selected randomly to be malicious nodes and two nodes are selected to be selfish nodes. Selfish nodes are configured to drop any packets that are requested to forward. And malicious nodes are configured to attack the neighbors by physical layer denial of service attack.

As we know, AODV can not detect selfish nodes and malicious nodes, such misbehaved nodes may leads to MAC layer, network layer or even transmission layer retransmission, which leads to low and unstable network throughput. The SARO-AODV protocols can detect and prevent such misbehaved nodes from degrading the network performance. Since, SARO-AODV relies on reputation system to evaluated node reputation, which is a relative slow process. As shown in Fig. 3, the throughput of SARO-AODV is slow in the first 10 sec. But after reputation evaluation process is finished, the throughput of the network keeps high and stable, selfish

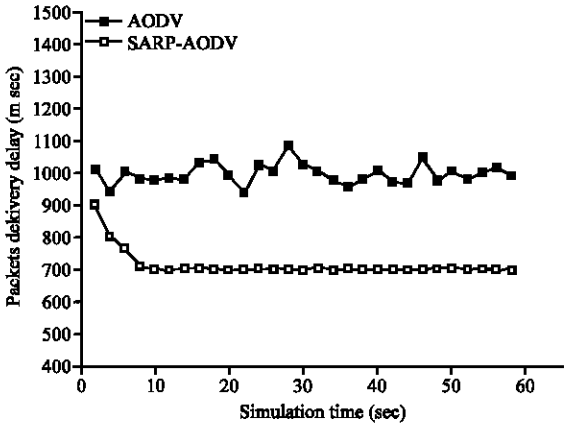

Fig. 4: Delay at MAC layer

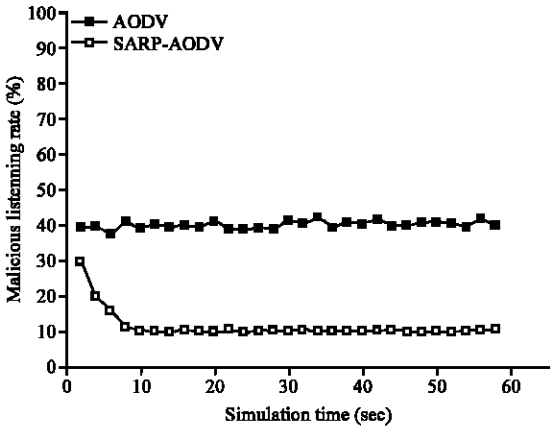

Fig. 5: Malicious listening rate

nodes and malicious nodes is isolated in SARO-AODV completely. The throughput of it is much higher than AODV.

Misbehaved nodes desterilize performance at MAC layer, network layer and transmission layer, which leads to retransmission at different levels. The transmission delay is a very important parameter for real time data transmission. And the second simulation cares about delay characters. The SARO-AODV can isolate both selfish and malicious nodes and reduce their impact on network performance. As shown in Fig. 4, the delay and its jitter are much lower as compared to that of AODV.

Malicious listening is dangerous for wireless network, which is usually a prelude of attacks. Reducing malicious listening is very important for security routing. We define malicious listening rate to be the rate of amount of captured packets by malicious packets to amount of all transmitted packets. Figure 5 shows malicious listening rate under different protocols. As mentioned above, SARO-AODV can isolate malicious nodes and its

neighboring nodes; the malicious listening rate is greatly reduced as compared to that of AODV.

CONCLUSION

As compared to wired network, wireless network is more frangible to attacks. And wireless ad hoc is especially prone to attacks as there are no center control nodes. Security on wireless ad hoc network is a hot research topic. Until now, there are no standards for security of ad hoc network. This study proposes a novel ACO based security routing scheme. Based on reputation systems, this scheme can isolate misbehaved nodes completely. Furthermore, this scheme deals with selfish nodes and malicious nodes different, which is more practical as compared to previous schemes. By a time sensitive adaptation of classical ACO, this scheme is more suitable for wireless security, which is characteristic by time variable channel and sudden attacks. Simulation results show that the scheme can protect the network effectively and improve the performance of network dramatically.

REFERENCES

Banerjee, S., C. Grosan and A. Abraham, 2005. IDEAS: Intrusion detection based on emotional ants for sensors. Proceedings of 5th International Conference on Intelligent Systems Design and Applications, Sept. 8-10, Department of Computer Applications, Institute of Manage, Studies, India, pp: 344-349.

Buchegger, S. and J.Y. Le Boudee, 2005. Self-policing mobile ad hoc networks by reputation systems. IEEE Commun. Mag., 43: 101-107.

Di Caro, G., F. Ducatelle and L.M. Gambardella, 2004. Ant Hoc Net: An ant-based hybrid routing algorithm for mobile Ad Hoc Networks. Proceedings of the 8th International Conference on Parallel Problem Solving from Nature PPSN VIII, Number 3242 in Lecture Notes in Computer Science, September 2004, Springer-Verlag Birmingham, UK., pp: 461-470.

Gerla, M., 2004. Mohapatra Ad Hoc Networks Technologies and Protocols. Springer Science Press, Boston, USA.

Gunes, M., U. Sorges and I. Bouazizi, 2002. ARA-The ant-colony based routing algorithm for MANETs. Proceedings of ICPP Workshop on Ad Hoc Networks, Aug. 18-21, IEEE Computer Society, Washington, DC, USA., pp: 79-85.

Gupta, V., S. Krishnamurthy and M. Faloutsos, 2002. Denial of service attacks at the mac layer in wireless ad hoc networks. Proceedings of MILCOM, Oct. 7-10, Anaheim, CA., pp: 1118-1123.

Günes, M. and O. Spaniol, 2003. Ant-Routing-Algorithm for Mobile Multi-Hop Ad-Hoc Networks. In: Network Control and Engineering for Qos, Security and Mobility, Gati, D. (Ed.). Kluwer Academic Publishers, New York, pp: 120-138.

Hussein, O. and T. Saadawi, 2003. Ant routing algorithm for mobile ad-hoc networks (ARAMA). Proceedings of the IEEE International Performance, Computing and Communications Conference, April 9-11, IEEE Computer Society, Washington, DC, USA., pp: 281-290.

Kennedy, J. and R. Eberhart, 2001. Swarm Intelligence. 1st Edn., Academic Press, San Diego, CA., ISBN: 1-55860-595-9.

Paul, K. and D. Westhoff, 2002. Context aware detection of selfish nodes in DSR based ad-hoc networks. Proceeding of IEEE Global Telecommunications Conference, Aug. 7-9, IEEE Computer Society, Washington, DC, USA., pp: 178-182.

Peha, J.M., 2000. Wireless communications and coexistence for smart environments. IEEE Wirel. Commun., 7: 66-68.