IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 4 Issue 5, May 2017
ISSN (Online) 2348 – 7968 | Impact Factor (2016) – 5.264
www.ijiset.com

Quantitative Assessment System for Reliable Routing in WSN

Mrs. Vani B[1], Dr. Shrishail Math[2], Mr. Mahesh B[3]

[1]Associate Professor, Department of C.S.E, Sambhram Institute of Technology, Bengaluru, Karnataka, India

[2] Professor, Head of Department, Department of I.S.E, Dayanand Sagar College of Engineering, Bengaluru, Karnataka, India

[3] Assistant Professor, Department of Computer science, Bangalore Technological Institute, Bengaluru, Karnataka, India

Abstract

Quantitative reliable assessment system is proposed to improve security and dependability of wireless sensor network. Ad hoc On-Demand Distance Vector (AODV) routing protocol is used to authenticate reliable routing system in wireless sensor network, Route Reply (RREP) Message is extended to record node residual energy assessment and attack behavior assessment. NS-2 simulator is used to simulate the reliable routing system under different network attack behaviors. Five kinds of node attack behaviors are used to evaluate and validate the reliable routing system. Simulation results show that reliable routing system can improve the security and performance of network. It shows better than other security system.

Keywords: *reliable, AODV, attack behavior, Assessment, simulation.*

1. Introduction

Wireless sensor networks (WSNs) are innovative wireless networks consisting of a number of sensor nodes with limited power, storage and communication [1]. The basic function of wireless sensor networks is to collect information for authorized users. WSN has little or no infrastructure. It consists of a number of sensor nodes working together to monitor a region to obtain data about the environment. WSNs have many potential applications such as military target tracking and surveillance and natural disaster rescue, biomedical health monitoring and hazardous environment exploration and seismic sensing.

Unlike traditional networks, WSN has its own design and resource constraints. Resource constraints include a limited energy, short communication range, low bandwidth, limited processing and storage in each node. As sensor nodes operate on limited battery power, energy usage should be considered in WSN. When a sensor node is depleted of energy, it will die and disconnect from the network which can significantly impact the network performance.

Sensor network lifetime depends on the number of active nodes and connectivity of the network, so energy must be used efficiently in order to maximize the network lifetime. The size of the network varies with the monitored environment. For indoor environments, fewer nodes are required to form a network in a limited space whereas outdoor environments may require more nodes to cover a larger area. Recently, reliable computing is attracted more and more attention in information security research. Reliable computing maybe needs the support of hardware architecture and embedded processor technology. Reliable and reputation have been recently suggested as an effective security mechanism for open environments such as sensor network.

The performance and security of sensor networks depend on reliable in distributed nodes. To enhance security in sensor networks, it is important to evaluate reliable worthy degree of nodes. To a single node, it's difficult to know whether to reliable the other nodes with its own information and knowledge, especial in routing discovery step, selecting a reliable path is important to build a security WSN network. Traditional security methods which provide confidentiality, authentication and availability are not efficient to sensor network because of the special network application scenarios.

Traditional cryptographic technology is difficult to process active attacks. Reliable is the degree of belief about the future behavior of other entities, which is based on the past experience of the nodes. To sensor network, if WSN nodes want to communicate or exchange key data, it is necessary to establish reliable relationship between nodes to ensure the reliable data exchange. Reliable is related to many factors, such as hop count、node behavior node's residual energy. In this paper, a novel reliable routing system is proposed. Multi-agents collect multi-factors information and cooperate to decide the reliable route.

2. Related Work

Blaze, Feigenbaum, and Lacy [2] firstly introduce reliable management as a separate component of security services and give an overall definition of the reliable management problem. The authors propose a unified decentralized reliable Management system, policymaker, which was based on a simple language for describing security policies, credentials and relationships. While the system is not fit to sensor network, because of the different network architecture.

New reliable system is necessary to the special characteristics of the sensor network. Reputation-based Framework for Sensor Networks (RFSN) [3] is the reputation and reliable-based model designed and developed exclusively for sensor networks, which using watchdog mechanism to build reliable rating. Each sensor node develops a reputation for each other node by making direct observations about the other neighbor nodes. This reputation is used to help a node evaluate the reliable worthiness of other sensor nodes and make decisions within the network. But the watchdog cannot record all the behavior due to its own fault or network error, so there is some uncertainty events in the reliable system.

Mutual entity authentication plays an important role in securing wireless sensor networks. Zhijun Li and Guang Gong propose a computationally efficient authentication framework [4], based on a well-studied problem—learning parity with noise (LPN). This kind of LPN-based authentication approach only involves simplest bit operations, which makes them suitable for resource restrained sensor nodes. The proposed framework introduces a new noise mode to prevent a general man-in-the-middle attack. Haiguang Chen and Huafeng propose agent-based reliable management model system to enforce the security of wireless sensor networks [5]. The agent nodes monitor the behavior of sensor nodes within its radio range to distribute the reliable rating. They don't need the second-hand information to build reliable system.

A novel multi-agent-based dynamic lifetime intrusion detection and response system [6] is proposed to combat the two types of attacks-Denial-of-service and Black hole attacks. Simulation results show that multi-agent-based dynamic lifetime security system is highly effective to detect and block the two kinds of attacks. It can efficiently improve reliable worthiness, decrease computing complexity and save energy consumption for network securities. Yonglin Ren and Azzedine Boukerche take advantage of a reliable system to prevent effectively the misbehavior of malicious nodes so that only reliable worthy nodes are allowed to participate in communications[7]. They present the Malicious Encryption and Malicious ID attacks, as well as other attacks, and note how their system is robust to them. They provide its performance assessment based on simulation experiments implemented in an ns-2 simulator.

Ming-Zheng Zhou and Yi Zhang propose a reputation model called BRMSN (Behavior Reputation Method for Sensor Networks) which focuses on local testing [8]. The model defines the similarity and the similarity matrix by using normal differences among status estimate vectors. The simulation results show that the model can reduce the number of data exchange among sensors, also the model has the powerful ability to prevent from malicious attacks or faulty nodes

DoS attacks for AODV routing protocol are classified and analyzed by Chen Hongsong and Fuzhongchuan[9].A novel intrusion detection system based on NP is proposed to com bat the attacks. The reliable worthy Agent can change its state with the AODV routing process to save energy. Agent can update itself to a higher reliable worthiness neighbor to keep the high reliable worthiness of network. Simulation results show that the attacks have great effect on the system performance. NEELI R. PRASAD and MAHBUBUL ALAM propose that different security levels can allow different WSN services [10].

The reason why different security levels were defined is to find the balance between two opposite tendencies. The first is to implement a high level of security, in order to provide the maximum protection to the transferred data, and the second is to give security a secondary role, in order not to affect the performance of network. This work proposes a solution based on the required level of security and implements the encounter security needs with the minimum burden for network's devices.

BinodVaidya and Dimitrios Makrakis introduce a comprehensive resilient security framework for wireless ad hoc networks that are using multipath routing[11]. It deploys an integrated multi-signatures system and uses a self certified public key system to ensure secure route discovery. In addition, it uses the Schnorr signature system along with an information dispersal algorithm to ensure secure data transfer. However, the method is high cost to wireless sensor network.

Ahmet Burak Can and Bharat Bhargava propose a Self-ORganizing Reliable model (SORT) that aims to decrease

malicious activity in a P2P system by establishing reliable relations among peers in their proximity [12].

Peers create their own reliable network in their proximity by using local information available and do not try to learn global reliable information. Two contexts of reliable, service and recommendation contexts are defined to measure reliable worthiness in providing services and giving recommendations.

3. AODV Routing Extension

Katsuhiro Naito and Kazuo Mori propose a simple power-aware routing protocol for sensor networks [14]. Their proposed protocol is based on the ad hoc on-demand distance vector (AODV) protocol, which is one of the reactive routing protocols. In addition, they introduce forwarder nodes in the sensor networks in order to extend the lifetime of the entire sensor network. In fact, AODV protocol can be used to both wireless sensor network and ad hoc network.

The Ad hoc On-Demand Distance Vector (AODV) algorithm enables dynamic, self-starting, multi-hop routing network. It offers quick adaptation to dynamic link conditions, low processing and memory overhead and determines unicast routes to destinations. It is an on demand algorithm, meaning that it builds routes between nodes only as desired by source nodes.

It maintains these routes as long as they are needed by the sources. Additionally, AODV forms trees which connect multicast group members. The trees are composed of the group members and the nodes needed to connect the members. AODV uses sequence numbers to ensure the freshness of routes. It is loop-free, self starting, and scales to large numbers of mobile nodes.

The Ad hoc On-Demand Distance Vector (AODV) algorithm enables dynamic, self-starting, multi-hop routing network. It offers quick adaptation to dynamic link conditions, low processing and memory overhead and determines unicast routes to destinations. It is an on demand algorithm, meaning that it builds routes between nodes only as desired by source nodes.

It maintains these routes as long as they are needed by the sources. Additionally, AODV forms trees which connect multicast group members. The trees are composed of the group members and the nodes needed to connect the members. AODV uses sequence numbers to ensure the freshness of routes. It is loop-free, self starting, and scales to large numbers of mobile nodes.

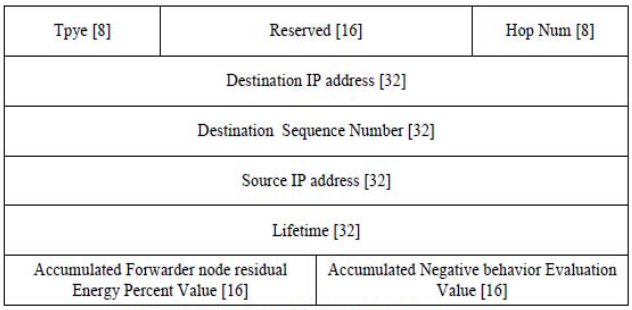

Fig.1 The Format of Extended Route Reply Message

The format of the extended route reply message is illustrated in figure 1, the extension regions include accumulated forwarder node residual energy percent value and accumulated negative behavior assessment value. Node energy agent computes current node's residual energy and percent value, then the agent accumulates the value in the RREP extension zone. Node behavior agent evaluates the attack behavior of previous node and accumulates it in the RREP negative behavior assessment value. Accumulated negative behavior assessment value expresses network attack condition. Reliable routing agent synthesizes routing reliable assessment value by reliable routing metrics, source node should choose high reliable worthy route by reliable routing system.

4. Simulation and Analysis

NS-2 simulator is a discrete event simulator targeted at wired and wireless networking research. Simulation with the tool ns-2 is widely used in sensor network research. In order to validate the reliable routing system, AODV routing protocol is extended in NS-2 to evaluate it. We use continuous bit rate (CBR) in all our experiments.

In network simulation scenario, there are 5 mobile nodes in the previous experiments. The field configuration is 100 m × 100 m. The simulation runs for 500 seconds. In a node's transmission range (25m), other nodes can receive signals from this node. The physical link bandwidth is 2 Mbps. Table 1 shows the simulation parameters configuration.

Table 1 Simulation parameters

Communication Type	CBR
Number of Nodes	5
Simulation Area	100m*100m
Simulation Time	500 seconds
Packet Rate	5 pkt/sec
Number of Connections	1
Transmission Range	25m
Physical Link Bandwidth	2Mbps

Different network scenarios are designed to validate reliable routing framework, there are two different energy nodes in the first scenario, there are two different node behavior in the second and third scenarios, there are two attack nodes in composed attack scenarios. To record different node behaviors, node behavior record table is created and saved in every node. The table will be used for reliable routing agent. Table 2 shows the structure of node behavior record table.

Table 2 Node behaviour record table

Node behaviour	Node Attack Behaviour type	Node Behaviour evaluation increment value	Behaviour weight-- W1
attack behaviour	The number of reaction attack	1	0.1
	The number of active attack	2	
	The number of composed attack	4	

As shown in table 2, there are three types of node attack behaviors. Node behavior record table items are implemented by linear list data structure. Node attack behavior includes reaction attack behavior、active attack behavior and composed attack behavior. Node behavior assessment value is increased by different type of attack behavior. The number of attack can be recorded in the table. Attack behavior weight is 0.1.The structure can be realized easily. Node attack behaviors can be recorded in the table by node behavior agent.

In wireless sensor network, because of cooperation character of the network, node behavior can influence the network performance greatly. Node attack behavior can decrease the network performance. In the paper, node attack behaviors include reaction attack behavior active attack behavior and composed attack behavior, in which composed attack behaviors include multi-node time division attack and multi-node task division attack, the multi-node task division attack includes two attack method. So five kinds of attack behavior are simulated and evaluated in this paper.

4.1 Simulation of Node Composed Attack Behavior

To research multi-nodes cooperate attack behavior, the Complex simulation scenario is designed, the network Scenario is shown in figure 5.

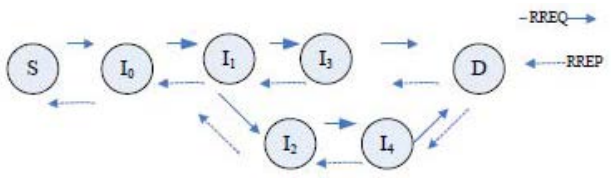

Figure 5. The Complex Simulation Scenario

In the figure 5, node I1 and node I3 can cooperate to attack the network. Node I0 、 node I2 and node I4 are normal nodes. In this paper, multi-nodes composed attacks include multi-nodes time division attack and multi-nodes task division attack. In the complex simulation scenario, multi-nodes time division attack refers to the node I1 and I3 attack the network by different time slice; multi-nodes task division attack refers to the node I1 and I3 execute different attack task by sending different route control packet.

In multi-nodes time division attack, node I1 and I3 attack the network by different time slice, node I1 first sends the fake RREP message, reliable routing system can compare the source IP address of the node to the source IP address of RREP message, the hop number is one, while the two addresses are different, so malicious node I1 can be detected and isolated by reliable AODV system.

Then the node I3 sends the fake RREP message at the second time slice, it can be detected and isolated by reliable routing system at the same method. Figure 6 shows the performance assessment of reliable AODV system under multi-nodes time division attack behavior.

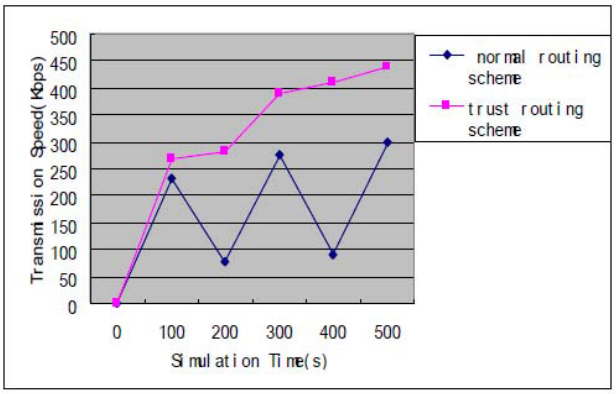

Figure 6. Performance assessment of reliable AODV system under multi-nodes time division attack

Seen from the figure 6, node I1 sends fake RREP message from 100s-200s,node I3 sends fake RREP message from 300s-400s. As node I1 and node I3 attack the network in different time slice. Multi-nodes time division attack influences the network performance periodically. Packet transmission speed between node S and node D also decreases periodically. The attack can be detected by node behavior agent and reported to reliable routing agent. Then network performance can be improved in reliable routing system. So reliable routing system can counter the composed
attack behavior effectively.

In multi-nodes task division attack, node I1 and I3 cooperatively attack the network by sending different routing control packet. There are two different kinds of task-division attacks in this paper. In the first multi-nodes task division attack, node I1 sends fake Route Error message to disrupt the normal route, then I3 sends fake RREQ message to declare it is source node S.

In the second multi-nodes task division attack, node I1 sends fake Route Error message to disrupt the normal route, then I3 sends fake RREP message to declare it is destination node D. In the first multi-nodes task division attack, node I1 broadcasts Route Error message to declare that the routing between node S and node D is interrupted, then node I3 sends fake RREQ message to declare that it is node S. Then the normal network traffic between node S and node D reduces.

The transmission speed between node S and node D decreases greatly. In fact, normal traffic between node S and node D transfers to the traffic between the node I3 and node D. In normal AODV routing system, the task division attack cannot be detected. While in reliable routing system, node behavior agent can detect node I1 and node I3's fake message attack behavior. The malicious behavior can be detected by node behavior agent and reported to reliable routing agent. Then node I1 and I3 can be isolated to the network. Figure 7 shows the performance assessment of reliable AODV system under the first multi-nodes task division attack behavior.

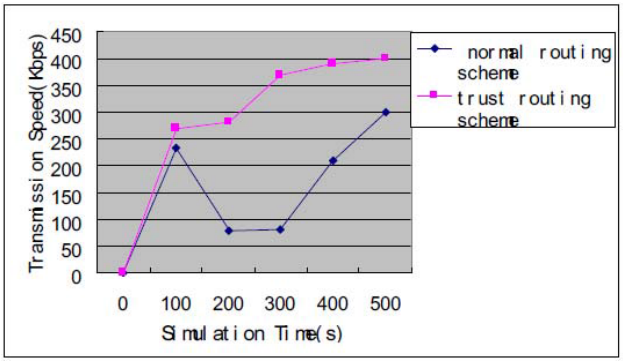

Figure 7. Performance assessment of reliable AODV system under the first Multi-nodes task division attack

Seen from the figure 7, node I1 sends fake Route Error message from 100s, then node I3 sends fake RREP message from 200s-300s. Multi-nodes task division attack influences the network performance greatly, packet transmission speed between node S and node D decreases when the attack happens. While the attack can be detected by node behavior agent and reported to reliable routing agent. Then network performance can be improved in reliable routing system.

In the second multi-nodes task division attack, node I1 broadcasts fake Route Error message to declare that the routing between node S and node D is interrupted, then node I3 sends fake RREP message to declare that it is node D. Then the normal network traffic between node S and node D reduces. The transmission speed between node S and node D decreases greatly. In fact, normal traffic between node S and node D transfers to the traffic between the node I3 and node D.

In normal AODV routing system, the task division attack cannot be detected. While in reliable routing system, node behavior agent can detect node I1 and node I3's fake message attack behavior. The malicious behavior can be detect by node behavior agent and reported to reliable routing agent. Then node I1 and I3 can be isolated to the network. Normal routing through node2 and node4 can be created. Figure 8 shows the performance assessment of reliable AODV system under the second multi-nodes task division attack behavior.

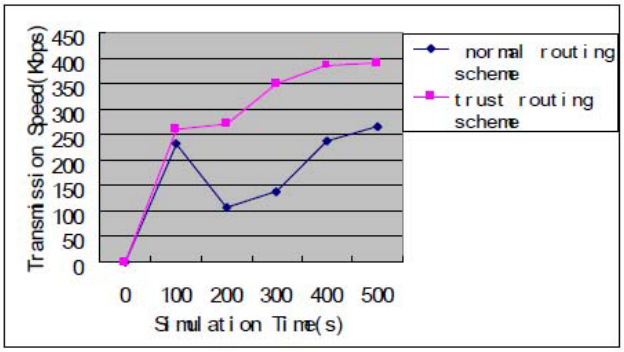

Figure 8. Performance assessment of reliable AODV system under the second multi-nodes task division attack

Seen from the figure 8, node I1 sends fake Route Error message from 100s, then node I3 sends fake RREP message from 200s-300s. Multi-nodes task division attack influences the network performance greatly, packet transmission speed between node S and node D decreases when the attack happens. While the attack can be detected by node behavior agent and reported to reliable routing agent. Then network performance can be improved in reliable routing system.

5. Comparison with legacy security systems

A novel reliable routing system is proposed in this paper, different node behaviors are evaluated in the reliable routing system, reliable agent can synthesize the

information from node energy agent and behavior agent. Reliable routing system can make the WSN more secure and intelligence. NS-2 simulator is extended to validate different experiment scenarios. Simulating results show that reliable routing system can improve WSN security and performance. The main contributions of this paper are the following two aspects:

(1) A quantitative reliable worthy routing assessment system for wireless sensor network is proposed in the paper. Definition and simulation of reliable routing is given in the paper. Node behavior record table structure is proposed to implement reliable routing system. Node energy and behavior are monitored by node energy agent and node behavior agent; the monitoring results are reported to reliable routing agent.

(2) Five different types of node attack behaviors are simulated and evaluated. They are reactive attack, active attack, multi-nodes time division attack, multi-nodes task division attack. In which multi-node task division attack includes two different attack conditions. Simulation results Show that the reliable routing system shows better performance than normal routing system in wireless sensor network.

References

[1] Jennifer Yick, Biswanath Mukherjee and Dipak Ghosal.Wireless sensor network survey. Computer Networks. 2008, 52(12):2292-2330
[2] M. Blaze, J. Feigenbaum, and J. Lacy. Decentralized reliable management. In Proceedings of the 1996 IEEE Symposium on Security and Privacy: 164-176
[3] S. Ganeriwal and M. Srivastava. Reputation-based framework for high integrity sensor networks. In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN '2004): 66-77
[4] Zhijun Li and Guang Gong. Computationally efficient mutual entity authentication in wireless sensor networks. Ad Hoc Networks.2011,9(2): 204-215
[5] Haiguang Chen and Huafeng Wu. Agent-based Reliable Management Model for Wireless Sensor Networks. International Conference on Multimedia and Ubiquitous Engineering, 2008:150-155
[6] Chen Hongsong, Ji Zhenzhou, Hu Mingzeng. Design and performance assessment of a multi-agent-based dynamic lifetime security system for AODV routing protocol .Journal of Network and Computer Applications. 2007, 30(1):145~166
[7] Y. L. Ren and A. Boukerche. ARMA: a scalable secure routing protocol with privacy protection for mobile ad hoc networks.Wireless Communications & Mobile Computing, 2010 vol. 10, no. 5: 672-687
[8] Ming-Zheng Zhou, Yi Zhang. A Reputation Model Based on Behavior Reliable inWireless Sensor Networks. Proceedings of the 2009 International Conference on Scalable Computing and Communications:188-194
[9] Chen Hongsong, Wang Zhaoshun, Zeng Guangping and Liu Hongwei. Using Network Processor to Establish Reliableworthy Agent System for AODV Routing Protocol.Wireless Personal Communications, 2007, Volume 42, Number 1:49-62
[10] Neelir. Prasad and Mahbubul Alam. Security Framework for Wireless Sensor Networks. Wireless Personal Communications (2006) 37: 455–469
[11] BinodVaidya, Dimitrios Makrakis, JongHyukPar and Sang-Soo Yeo. Resilient Security Mechanism for Wireless Ad hoc Network.Wireless Personal Communications (2011) 56:385–401
[12] Ahmet Burak Can and Bharat Bhargava. SORT:A self-organizing reliable model for per-to-peer systems. IEEE Trans. Dependable Sec. Comput. 2013,10(1): 14-27
[13] Pelin Angin and Bharat Bhargava. An Agent-based Optimization Framework for Mobile-Cloud Computing. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications. 2013,4(2): 1-17
[14] Katsuhiro Naito, Kazuo Mori, Hideo Kobayashi. Assessment of Power-Aware Routing for Sensor Networks with Forwarder Nodes.Journal of Systemics, Cybernetics and Informatics, 2008,6(5): 87-92 3-5