ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Secure Authentication Technique for Wireless Sensor Networks with Load-Balancing Routing Protocol

Kavitha H L [1], K N Pushpalatha [2]

P G Student, Department of Digital Electronics and Communication, Dayananda Sagar College of Engineering, Visvesvaraya Technological University, Bengaluru, Karnataka, India [1]

Associate Professor, Department of Electronics and Communication Engineering, Dayananda Sagar College of Engineering, Visvesvaraya Technological University, Bengaluru, Karnataka, India [2]

ABSTRACT: Wireless sensor networks are widely used in many applications and the complexity of the design and development of such applications is a challenging task. Hence service-oriented architectures are used to overcome these challenges which act as a middleware in WSN. Service-oriented architecture in WSNs is proposed so that new applications are developed fast by combining the services. Multipath routing schemes in WSNs are used to provide efficient traffic distribution but the failure of links might affect the reliability, scalability, security and performance of the network. In order to overcome these, it is desirable to design a fault-tolerant and efficient routing scheme. In this paper, a secure authentication and an efficient load balancing algorithm is proposed which improves the throughput of the network and improves the lifespan of the network. Simulations demonstrate the secure load balancing routing scheme.

KEY WORDS: Service-oriented architecture, Secure Authentication, Load balancing, Wireless sensor networks (WSNs).

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are widely used in many applications today. The wireless sensor networks are capable of acquiring data and modify it according to a particular application and communicate with the physical world [1]–[5]. For a particular application, a separate WSN is setup. This becomes more difficult as the request for new applications increases as a new network must be setup every time and these networks lack the standard operations and representation for sensor data which can be used by other services or upper layer applications. In order to overcome this complexity, service-oriented architecture for WSNs is proposed [4], [6]. This set of architectural concepts split the functions into definite units called services [7], [8], which can be distributed over a network and can be associated and recycled to create new applications. Major benefits of this approach are modularity, flexibility, loose-coupling and interoperability.

Service-oriented architecture rationally thinks that for user applications, WSNs as service provider. Through a set of services required by the WSN applications, the service-oriented architecture gives the idea for the complex underlining WSN. Such services can be data aggregation, security, adaptation, reliability, self-organization and management services. All these services and many other enhanced services can be designed using service-oriented architecture in order to provide an easy and adaptable environment to develop efficient WSN applications. In many application domains, services provide a set of explicit functions on the basis of the essential application logic that is distinct for each service and application. Nevertheless, those services and service providers must are also required to support certain common functionalities that are usually inappropriate to the main applications.

DOI: 10.15680/ijircce.2015.0306030

Traffic is traded on a huge scale in WSNs, as a result; how to increase the throughput of the WSNs is a crucial challenge in the design of service-oriented WSNs. Recently, many routing protocols are used for data transmission. Here we propose an adaptive multipath routing. Multipath routing allows formation of multiple paths connecting a single source and a single destination. Adaptive multipath routing is used to improve the reliability of data transmission or to accommodate load balancing which actively support QoS requirements. Every node on a path in WSN must be able to estimate the performance of its next hop neighbors regarding to the reliability of the path [7]. This routing scheme must be able to accommodate services with multipaths which are bandwidth guaranteed. Such multipaths support these services to be run over secure and reliable network architecture. Link-disjoint based multipath routing is a good scheme to deal with each application as a service task which can be supported by additional flexible protocol design and resource management. Every node must be able to identify the service-related nodes and forward the routing messages to them [2], [3]. In this paper, we propose an adaptive and secure load balancing routing method which improves the network performance for service-oriented WSNs.

II. RELATED WORK

In WSNs, designing a routing scheme is the most difficult challenge as the links between the nodes are unstable. Hence the routing scheme should be built such that the nodes must be able to sense, process and then transmit information. In order to obtain this a large number of routing schemes are proposed [9] - [13]. The multipath routing scheme must be able to contribute high aggregation bandwidth and fault tolerance and balance the load on multipaths. Hence a robust multipath is essential to offer reliable and robust transmission over multipaths [10], [11].

A.Valera proposed a new algorithm named CHAMP (CacHing And Multiple Path) which uses cooperative packet caching and shortest multipath routing in order to reduce the packet loss due to recurrent route failures. These two techniques produce appreciable improvements regarding end-to-end delay, packet delay, and routing overhead. This proposed protocol also proves that it is more efficient compared to other protocols in reducing packet loss due to repeated route failures [12]. D. Jurca explained the problems of selecting the efficient streaming policy for distortion optimal multipath video delivery, under delay constraints. A simple streaming model is introduced which considers the importance of video packet, and the dependencies among the packets and permits to process the quality perceived by the receiver, as a function of the streaming policy. He proposed a fast heuristic- based algorithm that provides an optimal performance compared to common scheduling algorithms and represents very efficient multipath streaming strategies for both stored and live video services [13].

S. Li proposed a compressed sensing (CS)-based framework for the Internet of Things(IoT) , where the end nodes measure, transmit, and store the sampled data in the framework. Then for in-network compression, an efficient cluster sparse reconstruction algorithm is proposed aming at more accurate data reconstruction and lower energy efficiency [14]. K.K Mamidisetty proposed a scalable approach for broadcasting that exploits all the shortest paths between a pair of nodes and improves QoS. Although multiple shortest paths are present in a system, it is shown that by spreading the messages over the multipaths in a Round-Robin manner these paths cannot be exploited. By modeling the multihop propagation in mesh topology as a multistage queuing, from a variety of scenarios they show that the proposed achieves improved QoS [15].

S.J. Lee proposed a scheme in order to improve existing on-demand routing protocols by generating a mesh and providing multiple alternate routes. This algorithm builds mesh and multipath without transmitting any additional control messages. This scheme is applied to the Ad-hoc On-Demand Distance Vector (AODV) protocol and the performances are compared [16]. W. Lou proposed a hybrid multipath scheme (H-SPREAD) to improve both reliability and security potentially unfriendly and unreliable wireless sensor networks. This scheme is based on a distributed N-to-1 multipath discovery process. Later a hybrid multipath data collection scheme is proposed. This scheme is very efficient in improving both security and reliability of the data collection service flawlessly.[17]

III. PROPOSED APPROACH

SA-AODV

In this paper, we propose an adaptive and secure load-balancing multipath routing protocol which is based on AODV, i.e. Secure Authentication AODV (SA-AODV) which includes following features.

1) **Packet Delivery Scheme**: It is the first stage of SA-AODV. Since data is being transmitted over multipaths, we need a secure data delivery scheme in order to avoid the packet loss during transmission. In service-oriented WSNs, this boosts the data confidentiality.

2) **Authentication**: After the multipath discovery, whether the nodes on each path are active and if any malicious nodes are present is verified during authentication process. If a malicious node is present, then it noted in the malicious_table and an alternate path from source to destination is determined.

3) **Load Balancing**: This is the last and important stage. Data is transmitted over the multipaths by the source to the destination, during which there might be a chance where the load on any path may exceed the capacity of node which leads to loss of data. In order to avoid this, load balancing algorithm is used. We use local fault information signals (FIS) for balancing the load.

A. PACKET DELIVERY SCHEME

We use threshold secret sharing algorithm in order to divide the data into many fragments. Every fragment is packed into an AODV packet, as shown in Fig 1. The data can be exactly recovered from any received T out of N packets where N is the number of packets the data is split into. This is called a (T, N) threshold secret sharing algorithm [18], [19], [20] where T is the threshold. The data of sent packets cannot be recovered if the packets received at the destination are less than the threshold.

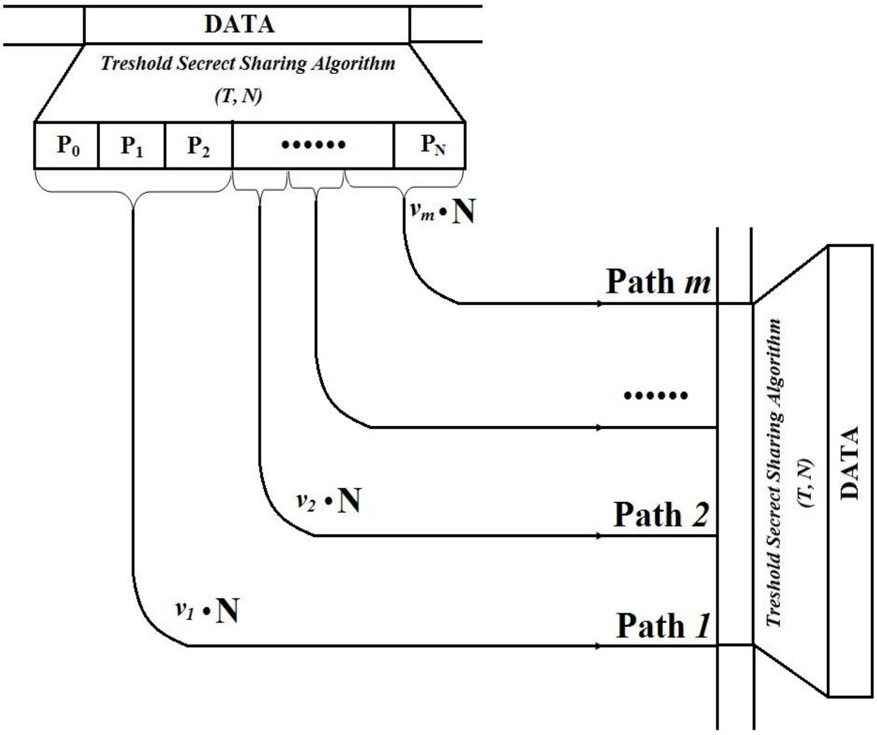

Fig 1. Packet Delivery Scheme.

B. AUTHENTICATION

Authentication process is done to check the conditions of the nodes i.e. malicious or not, across multipaths in WSNs. This process helps to avoid unnecessary data transmission to those node which are faulty which in turn reduces the delay and improves the efficiency and reliability of the network. Initially authentication process is carried out in order to find the malicious node if any present in the network. The procedure is as shown in Fig 2. If any malicious node is present in the network which is considered as grey hole node, then the grey hole removal process is initiated. The grey hole removal process is as shown in Fig 3. Once the authentication process is completed the malicious node will be added to the malicious table and this information is sent to all other nodes so that they avoid communications with that node.

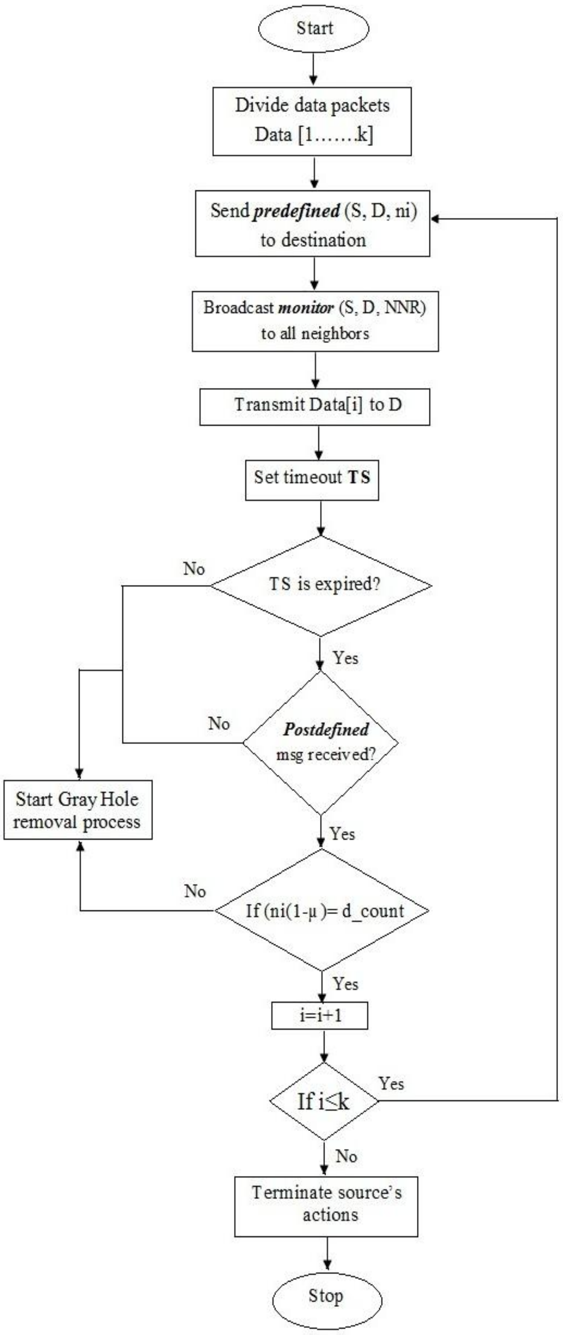

Fig 2. Authentication

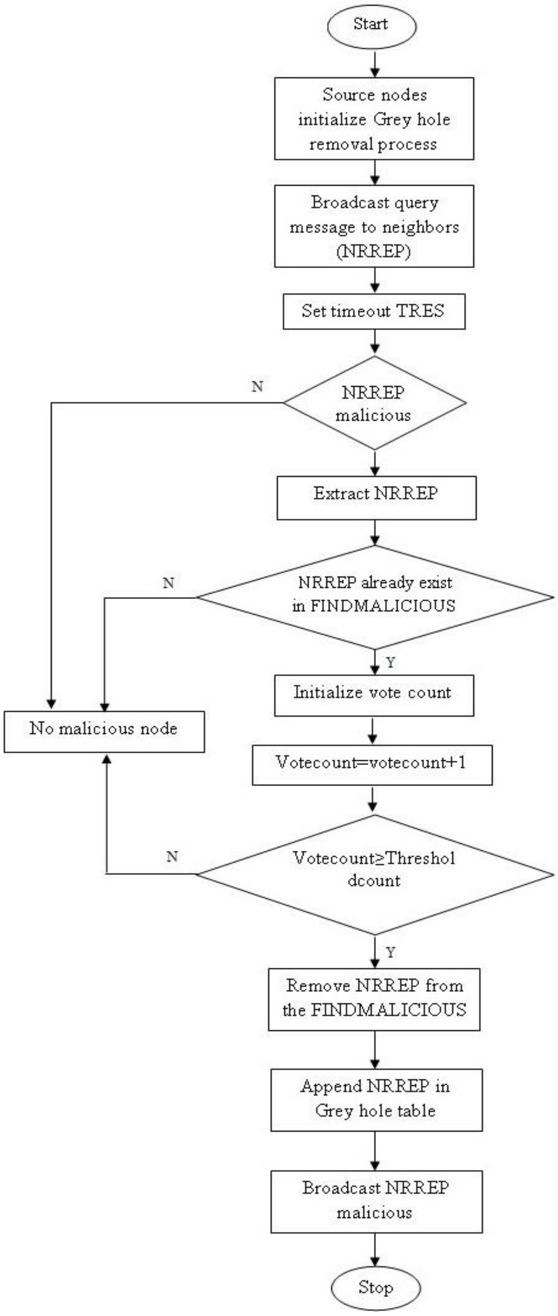

Fig 3. Grey Hole removal process

C. *LOAD BALANCING*

Load Balancing is the important part of SA-AODV. Data is transmitted over the multipaths by the source to the destination, during which there might be a chance where the load on any path may exceed the capacity of node which leads to loss of data. In order to avoid this, load balancing algorithm is used. We use local fault information signals (FIS) for balancing the load.

1) Fault signal is generated at the nearby node when load is excess.
2) Neighboring node sends fault information to other nodes in the network.
3) Since local signal is used to transmit the fault information, it is called Local Fault Information Signal (FIS).
4) Load is balanced based on the local FIS signal.

IV. SIMULATION RESULTS

NS-2 is an event simulator that supports simulation of TCP, routing and multicast protocols over wired and wireless networks. The proposed algorithm is implemented in NS2. The simulation topology includes the network with 50 sensing nodes. The simulation parameters were set as shown in Table 1.

Table 1: Simulation Parameters

Simulation Parameter	Value
Simulation Area	1000 m x 1000 m
Number of nodes	Mobile nodes = 50
Transmission Range	350 m
Traffic Flow	CBR
Transmission Power	0.2 mW
Reception Power	0.1 mW
Simulation time	3 min for each run

A network with 50 sensor nodes is setup and when the communication between these nodes starts, since authentication process occurs constantly using the secure authentication algorithm, the malicious node if any present in the network is found by using the secure authentication algorithm as shown in Fig 4. This malicious node is capable of eavesdropping to other neighboring nodes during their transfer of data as shown in Fig 5. Later this malicious node is either removed from the network or added to the malicious table in order for other neighboring nodes to know that it is a malicious node so that they avoid transmission of data to this node which results in data loss.

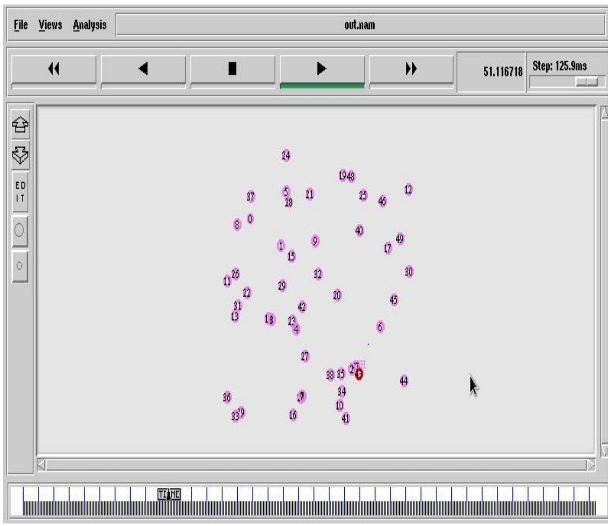

Fig 4. Malicious node present in the network.

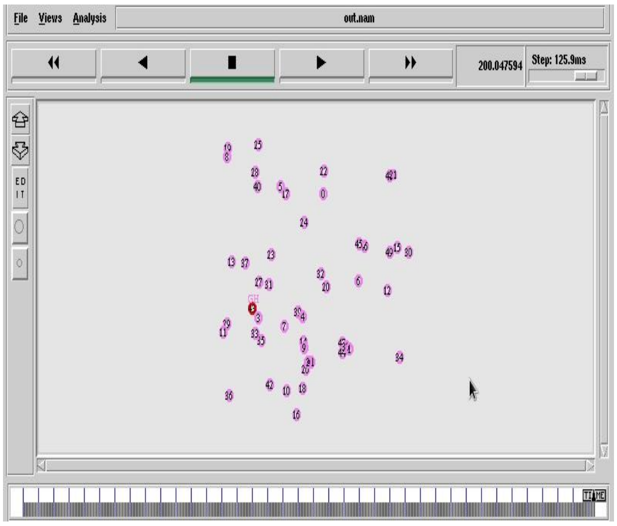

Fig 5. Malicious node eavesdropping to other nodes.

V. CONCLUSION

An adaptive load-balancing routing protocol (SA-AODV) is developed for WSNs that uses secure data delivery and load balancing in order to overcome the existing difficulties in the WSNs. SA-AODV uses a secret data delivery scheme which reduces packet loss and delay in the network. Each node in the network is authenticated continuously in order to find malicious node if any present. Even though this is an overhead this helps to avoid the failure of links which results in data loss. Load is balanced adaptively at each node which improves the reliability of the network.

REFERENCES

1. S. Li, X. Wang, and S. Zhao, "Multipath routing for video streaming in wireless mesh networks," Ad Hoc Sens. Wireless Netw., vol. 11, no. 1/2, pp. 73–92, 2011.
2. T. Zhao, K. Yang, and H.-H. Chen, "Topology control for service-oriented wireless mesh networks," IEEE Wireless Commun., vol. 16, no. 4, pp. 64– 71, Aug. 2009.
3. K. Lin, J. J. P. C. Rodrigues, H. Ge, N. Xiong, and X. Liang, "Energy efficiency QoS assurance routing in wireless multimedia sensor networks," IEEE Syst. J., vol. 5, no. 4, pp. 495–506, Dec. 2011.
4. A. Rezgui and M. Eltoweissy, "µRACER: A reliable adaptive servicedriven efficient routing protocol suite for sensor-actuator networks," IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 5, pp. 607–622, May 2009.
5. X. Zhang and H. Su, "Network-coding-based scheduling and routing schemes for service-oriented wireless mesh networks," IEEE Wireless Commun., vol. 16, no. 4, pp. 40–46, Aug. 2009.
6. L. D. Xu, "Enterprise systems: State-of-the-art and future trends," IEEE Trans. Ind. Informat., vol. 7, no. 4, pp. 630–640, Nov. 2011.
7. L. Duan, W. Street, and E. Xu, "Healthcare information systems: Data mining methods in the creation of a clinical recommender system," Enterprise Inf. Syst., vol. 5, no. 2, pp. 169–181, May 2011.
8. K. Wang, X. Bai, J. Li, and C. Ding, "A service-based framework for pharmacogenomics data integration," Enterprise Inf. Syst., vol. 4, no. 3, pp. 225–245, Aug. 2010.
9. Y. H. Yin, J. Y. Xie, L. D. Xu, and H. Chen, "Imaginal thinking-based human–machine design methodology for the configuration of reconfigurable machine tools," IEEE Trans. Ind. Informat., vol. 8, no. 3, pp. 659– 668, Aug 2012.
10. J. Guo, L. D. Xu, G. Xiao, and Z. Gong, "Improving multilingual semantic interoperation in cross organizational enterprise systems through concept disambiguation," IEEE Trans. Ind. Informat., vol. 8, no. 3, pp. 647–658, Aug. 2009.
11. X. Li, Z. Jia, P. Zhang, R. Zhang, and H. Wang, "Trust-based on-demand multipath routing in mobile ad hoc networks," IET Inf. Security, vol. 4, no. 5, pp. 212–232, Dec. 2010.
12. A. C. Valera, W. K. G. Seah, and S. V. Rao, "Improving protocol robustness in ad hoc networks through cooperative packet caching and shortest multipath routing," IEEE Trans. Mobile Comput., vol. 4, no. 5, pp. 443– 357, Sep./Oct. 2005.
13. C. Li, J. Zou, H. Xiong, and C. Chen, "Joint coding/routing optimization for distributed video sources in wireless visual sensor networks," IEEE Trans. Circuits Syst. Video Technol., vol. 21, no. 2, pp. 141–155, Feb. 2011.
14. S. Li, L. Xu, and X. Wang, "Compressed sensing signal and data acquisition in wireless sensor networks and Internet of things," IEEE Trans. Ind. Informat., 2013, to be published, DOI: 10.1109/TII.2012.2189222.
15. K. K. Mamidisetty, M. Duan, S. Sastry, and P. S. Sastry, "Multipath dissemination in regular mesh topologies," IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 8, pp. 1188–1201, Aug. 2009.
16. S. J. Lee and M. Gerla, "AODV-BR: Backup routing in ad hoc networks," in Proc. IEEE Wireless Commun. Netw. Conf., 2000, vol. 3, pp. 1311–1316.
17. W. Lou and Y. Kwon, "H-SPREAD: A hybrid multipath scheme for secure and reliable data collection in wireless sensor networks," IEEE Trans. Veh. Technol., vol. 55, no. 4, pp. 1320–1330, Jul. 2006.
18. W. Lou and K. Ren, "Security, privacy, and accountability in wireless access networks," *IEEE Wireless Commun.*, vol. 16, no. 4, pp. 80–87, Aug. 2009.
19. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, pp. 612–613, Nov. 1979.
20. Q.Wang, C.Wang, K. Ren,W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 5, pp. 847–859, May 2011.

DOI: 10.15680/ijircce.2015.0306030