Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 6, June 2015, pg.1154 – 1157

RESEARCH ARTICLE

Design of Secure Encryption Multipath AODV Protocol for Wireless Sensor Network

Nagaraj M. Lutimath

Department of Computer Science and Engineering, Sri Venkateshwara College of Engineering, Bangalore, India

n_lutimath@yahoo.co.in

Abstract—Network Security is more important in all areas. The data that is transferred must be retrieved securely. For secure data retrieval we use cryptographic solutions. Multipaths routing schemes in Wireless Sensor Networks (WSNs), have established the efficiency of traffic distribution over multipath to fulfill the quality of service requirements of applications. However, the failure of links might considerably affect the transmission performance, scalability, reliability, and security of WSNs. Thus, by considering the reliability, congestion control, and security for multipath, it is desirable to design a reliable and service-driven routing scheme to provide efficient and failure-tolerant routing scheme. We propose a Secure Multipath Encryption AODV (SMEAODV) protocol with path vacant ratio that uses an Attribute Based Encryption (ABE) algorithm, to evaluate and discover a set of node-disjoint paths from all available paths with security. A load-balancing metric with congestion control that can adaptively adjust the load over multipaths is extensively used. A threshold sharing algorithm with path vacant ratio is applied to divide the packets into many segments that will be delivered via multipath to the destination.

Keywords— WSN, AODV, ABE, load-balancing, reliability, scalability

I. INTRODUCTION

Network security is an important characteristic of a network. It prevents the information in a network from unauthorized access. It involves the authorization of access to information throughout a network and it is measured by network administrator. The need for security is to protect the information as well as provide authentication and access control for resources, guarantee availability of resources. Exploitation of WSNs applications has transformed the means to obtain information and interact with the physical world [1]–[5].Service-oriented architectures for WSNs have been proposed to support the interoperability between different applications [6]. The services provided by WSNs are data processing, data aggregation and localization services [7], [8]. The service-oriented WSNs aim to combine scalable wireless sensor technology with independent applications which are treated as services that can support via more flexible protocol design and resource management [4]. The generic and application-specific WSNs can help the service-oriented architecture and avoid majority of their limitations [9]–[11].

Some of the metrics in service-oriented applications are bandwidth, delay, load balancing, and reliability where each node provides the quality-of-service (QoS) parameters associated with these services [12], [13]. In a service-oriented WSN, applications can be designed over service requirements to depart from current application-specific or generic WSNs [4]. A large volume of traffic is exchanged over WSNs; as a result, how to

improve the throughput of WSNs is a critical challenge in the design of service-oriented WSNs. It is desirable to design an secure multipath routing scheme that is able to reduce the downstream traffic and dynamically support QoS requirements, as well as achieve reliable paths from a source node to a destination node. Each node on a path should be able to evaluate the performance of its next-hop neighbors according to the reliability of the path [7]. The multipath routing scheme should be able to provide the services with bandwidth guaranteed multipaths, which help these services be run over secure and reliable network architecture.

Existing multipath routing protocols generally do not exploit the service-oriented architecture over WSNs. Node-disjoint-based multipath routing is a good idea to treat each application as a service task that can be supported via more flexible protocol design and resource management. The service oriented WSNs should avoid forwarding routing messages to unrelated nodes. Each node should be able to detect service related nodes and forward to them the routing message. We propose a multipath routing scheme with features the following: 1) Secure data delivery; 2) Adaptive congestion control 3) Application independence and rate adjustment; and 4) Extensibility. It can be foreseen that the service oriented architecture is a promising approach for service-based applications in WSNs.

II. ATTRIBUTE BASED ENCRYPTION (ABE)

Attribute-Based Encryption (ABE) is vital cryptographic algorithm.. The secret key is based on a set of attributes. While decryption the set of attributes must match cipher text attributes.ABE has two types: Key-Policy ABE (KP-ABE), Cipher text-Policy ABE (CP-ABE). In Key-Policy ABE, the cipher text is encrypted with the attribute set. For decrypting, the policy is chosen by the key authorities. Fig 1 shows the ABE control access model for Attribute Based Encryption [14]. The End User consists of set of attributes. A subject is created by the user which contains the subject attributes. User Authorization is checked based on the user attributes and subject attributes, if the user is authorized he permitted to access the information, this is indicated by P in the diagram. An object with a set of attributes is also created for further processing.

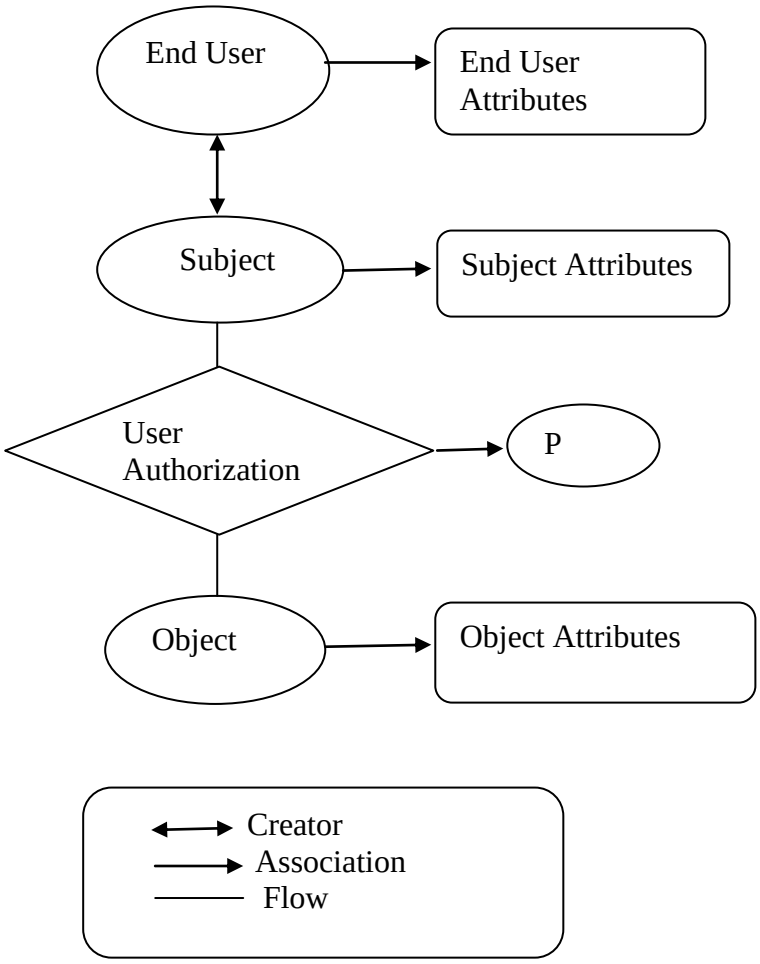

Fig -1: ABE based access control model

III. PROPOSED SCHEME

We will address challenges and present a secure and adaptive load-balancing multipath routing protocol based on AODV, namely, Secure Multipath Encryption AODV (SMEAODV), which includes the following features.

i. We use Attribute Based Encryption (ABE) algorithm for secure data delivery. Multipaths for reducing the delay of the packets. This first phase of our SMEAODV is used to improve the data privacy in the service-oriented WSNs, to separate the data packets using the path vacant ratio.

ii. A load-balancing approach that computes the path vacant ratio of multipaths is proposed for multipaths. The path vacant ratio can be used to evaluate the load over multipaths, which is derived from taking account of load balancing, path load, important paths, and importance of nodes over multipaths.

iii. The congestion control scheme adaptively adjust packet delivery rate over each path according to the congestion level that maintained by the HELLO message. Each intermediate node on active paths is able to adaptively detect the occurrence of congestion and then notify the parent nodes to reduce the packet delivery rate according to the congestion level.

Each node monitors its traffic load; when congestion occurs, it will update the congestion information in the HELLO message and then send the message to its parent nodes. The node will check its child nodes' congestion information when it receives a HELLO message. When it finds that the congestion level is too high, it will adjust the packet delivery rate on the path. By doing this, the long-term congestion can be prevented, which can further improve the throughput. The schematic block diagram of the proposed scheme is shown below.

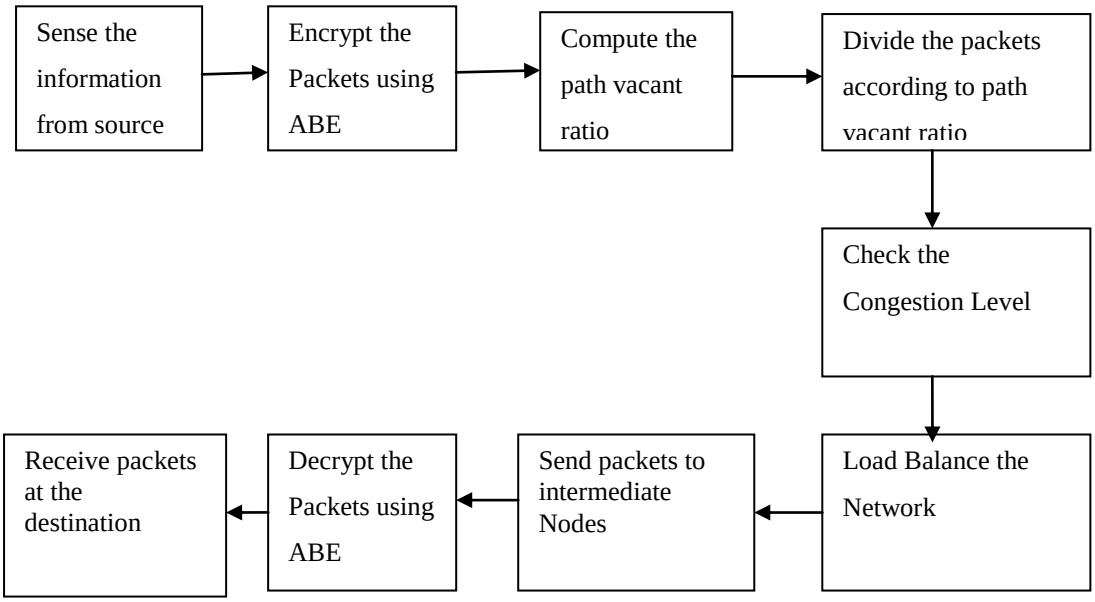

Fig 2: Block diagram of Proposed Scheme

Fig 2 shows the block diagram of the SMAODV protocol, the protocol uses node disjoint multipaths to form multipaths from a given source to destination. Path vacant ratio is used as evaluation metric for load balancing and formation of multipaths. Path vacant ratio V_i for i^{th} path is used for load balancing and is given by,

$$V_i = \frac{\sum_{i=1}^{N} PI(path_i) - PI(path_i)}{\sum_{i=1}^{N} PI(path_i)} \qquad (1)$$

In the equation (1), N is the total number of paths.

PI is the path importance of the node and is calculated by using the node connectivity degree of each sensor node.

The congestion control for multipaths includes three parts congestion detection, congestion control and notification, and load adjusting. In this phase, when a node receives CONGEST event. A CONGEST event is said to occur when a sensor node receives from its intermediate node a congestion message. When a CONGEST event occurs the sensor node first checks the value of CONGEST_LEVEL for each path. If the CONGEST_LEVEL is higher than one, i.e., two or three, it means that the load has to be adjusted according to the level value. The rules of adjustment are as follows. CONGEST_LEVEL = 1: It means that the load is normal

and each path is working well. CONGEST_LEVEL = 2: It means that the paths are congested on the node. It has to adjust the load by reducing the sending rate to the next lower rate. In our protocol, we use packet service ratio $r(i)$ to measure the congestion level at each node i, Packet service ratio is defined as the ratio of average packet service rate and packet scheduling rate.

Before congestion is checked the packets are encrypted using AES algorithm. The packets are divided using path vacant ratio and sent to intermediate nodes. A sensor node checks the congestion level and load balancing is done depending on the value of packet service ratio *r (i).*The packets are then decrypted using AES and received at the receiver.

IV. CONCLUSION

We have designed SMEAODV for WSNs that uses load balancing, congestion control and ABE algorithm. In SMEAODV, the packets are delivered across multipaths using a secure and reliable scheme. This improves the node's capabilities for applications and offers optimization alternatives which are not available in current schemes.

We have established the foundation for routing schemes over service oriented architecture, which is expected to have the same impact on sensor architectures. This design is expected to provide effective routing performance for multipath and enable WSNs to provide reliable application-level services. In further study we implement the proposed protocol using NS2 to know its efficiency based on network performance.

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. ½ 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 efficiencyQoS 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 forpharmacogenomics data integration," *Enterprise Inf. Syst.*, vol. 4, no. 3, pp. 225–245, Aug. 2010.

[9] D. Chiang, C. Lin, and M. Chen, "The adaptive approach for storage assignment by mining data of warehouse management system for distribution centres," *Enterprise Inf. Syst.*, vol. 5, no. 2, pp. 219–234,May 2011

[10] E. Xu, M. Wermus, and D. Bauman, "Development of an integrated medical supply chain information system," *Enterprise Inf. Syst.*, vol. 5,no. 3, pp. 385–399, Aug. 2011

[11] L. Duan and L. D. Xu, "Business intelligence for enterprise systems: A survey," *IEEE Trans. Ind. Informat.*, vol. 8, no. 3, pp. 679–687, Aug. 2012.

[12] L. D. Xu,W. Viriyasitavat, P. Ruchikachorn, and A.Martin, "Using propositional logic for requirements verification of service workflow," *IEEE Trans. Ind. Informat.*, vol. 8, no. 3, pp. 639–646, Aug. 2012.

[13] S. Li, L. Xu, X. Wang, and J. Wang, "Integration of hybrid wireless networks in cloud services oriented enterprise information systems,"*Enterprise Inf. Syst.*, vol. 6, no. 2, pp. 165–187, May 2012.

[14] Yang Ming, Liu Fan, Han Jing-Li, Wang Zhao-Li "An Efficient Attribu e based Encryption Scheme with Revocation for Outsourced Data Sharing Control", IEEE International Conference on Instrumentation, Measurement, Computer, Communication and Control, pp. 516-520,2011

