Volume: 04 Issue: 06 Pages:1793-1798 (2013) ISSN : 0975-0290

OSRWQOS: Optimized Secure Routing Protocol with QoS against Byzantine Attack

[1] K Sreenivasulu
Department of Computer Science & Engineering, Madina Engineering College, KADAPA, A.P. INDIA.
Email: sreenu.kutala@gmail.com
[2]Dr.E V Prasad
Rector, JNTUK, KAKINADA. A.P INDIA.
Email: profevprasad@yahoo.com
[3]Dr. A. Subramanyam
Department of Computer Science & Engineering AITS, Rajampet ,KADAPA. A.P INDIA.
Email: smarige@gmail.com

----------**ABSTRACT**----------

Several routing protocols have been proposed in recent years for possible deployment of Mobile Ad hoc Networks (MANETs) in military, government and commercial applications. Secure ad hoc networks are expected to meet five security requirements: confidentiality, integrity, authentication, non-repudiation and availability. Routing Algorithm that integrates security and performance requirements are considered to be more advantage. The SRAC protocol optimizes a combined objective function of security and performance parameters. However, the destination wait- time for decision on route selection and Trustworthiness–QoS index calculation at each node add up for delay. The use of two different routes and synchronization in the packets results with additional overhead. In this paper, an effective solution that overcomes the cons of SRAC is proposed with same security and better QoS can be achieved.
Keywords: MANET, Secure Routing, Byzantine Attack, QoS, AODV.

Date of Submission: March 13, 2013 Date of Acceptance: May 07, 2013

I. INTRODUCTION

Routing is one of the most basic networking functions in mobile ad hoc networks. It has been realized by many researchers for the need for secure routing protocols for ad hoc networks. The security of those protocols has been analyzed either by use of informal means, or with formal methods that have never been intended for the analysis of this kind of protocol. The attacks clearly demonstrate that flaws can be very subtle and, therefore, hard to discover by informal reasoning. In this a more systematic approach to analyze ad hoc routing protocols based on a rigorous mathematical model with precise definitions of security. Routing Algorithm dispenses the right route and then forwards the packets accordingly.

Each of these protocols differs in routing methodologies and use of information for routing decisions. At a very informal level, security of a routing protocol depends on how best it functions in the presence of an adversary that tries to prevent the correct functioning of the protocol. The a*ttacks on* ad hoc networks can be classified into two categories. The p*assive attacks* involve only *eavesdropping* of data and the a*ctive attacks* involve actions performed by adversaries, for this active attack may lead to replication, modification and deletion of exchanged data. *External attacks* are typically active attacks that are targeted e.g. to cause congestion, propagate incorrect routing information, prevent services from working properly or shut down them completely. External attacks can typically be prevented by using standard security mechanisms such as firewalls, encryption and so on. *Internal attacks* are typically more severe attacks, since malicious insider nodes already belonged to the network as an authorized party and are thus protected with the security mechanisms that the network and its services offer.

Ad hoc routing protocols must be integrated into authentication architectures, such as public key infrastructure (PKI) and certificate authority (CA), to achieve the security requirements including confidentiality, integrity, authentication, and no repudiation services. The main concerns for a secure routing protocol include

- To detect and defend internal attacks against routing protocols, among them Byzantine attacks proved to be a challenging problem.
- Identification of type of authentication and key management scheme to be adopted dynamically to maintain a trustworthy topology and defend against malicious attacks.

Volume: 04 Issue: 06 Pages:1793-1798 (2013) ISSN : 0975-0290

- To integrate the existing secure routing protocols first establish a PKI and then use cryptographic primitives to protect the messages exchanged. Security requires using intensive computations, whereas routing needs to be efficient to properly scale.
- To quantify the engineering tradeoffs between the security and performance requirements. The problem thoroughly so far has not well been investigated.

The Secure Routing Against Collusion (SRAC) proposed in [1] defend Byzantine attacks as other internal attacks optimizing QoS. This paper proposes a novel mechanism labeled Optimized Secure Routing Protocol with QoS (OSRWQOS), an improved method on a SRAC thatachieves not only good QoSand security, but also reduced add up delay at each node.

This paper is organized as follows. Related work is reviewed in Section II. An improved Dynamic Key management scheme is in Section III. The routing algorithm is briefed in Section IV and simulation results are related in Section V. Section VI concludes the paper.

II. Related Work

Byzantine attacks are the adversary and takes full control of an authenticated device and perform arbitrary behavior to disrupt the system [2]. Many Byzantine attacks of the features with the "selfish" node problem like not forwarding the data packets to others, but the intentions between these two are different. The goal of the selfish node is to reap the benefits of participating in the ad hoc network without having to expend its own resources in exchange. In contrast, the goal of the Byzantine node is to disrupt the communication of other nodes in the network, without regard to its own resource consumption. These cause Byzantine omission failures which include like failing to receive a request or failing to send a response and the commission failure to process a request incorrectly or to send an incorrect or inconsistent response to a request. Some of the Byzantine attacks are Black Hole attack, Gray Hole attack, Flood Rushing attack and Wormhole attack.

The two popular detection mechanisms Profile based detection and Specification based detection are described below [3] [5]:

Profile-based detection

Profile-based detection , known as behavior-based detection, defines a profile of normal behavior and classifies any deviation of that profile as an anomaly, with the assumption that attacks are events and distinguishable from normal legitimate system resources. Although this type of anomaly detectors are able to detect novel attacks, they are prone to high false positive rate due to the difficulty of clear segmentation between normal and abnormal activities and the use of insufficient or inadequate features to profile normal behaviors.

Specification-based detection

Specification-based detection defines a set of constraints that describe the correct operation of a program or protocol and monitors the execution of the program with respect to the defined constraints. It has been shown that specification-based techniques live up to their promise of detecting both known and unknown attacks, while maintaining a very low rate of false positives. Since, the increasing popularity of wireless networks on a wired networks, security is being considered as a major threat in them. Wireless network exposes a risk that an unauthorized user can exploit and severely compromise the network. So there is a need for secured wireless system to analyze and detect both passive & active attacks

In literature extensive work on secure routing protocols for MANETs and security mechanisms to existing popular on-demand & secured routing protocols, such as ad hoc on-demand distance vector routing (AODV), destination-sequenced distance vector (DSDV), and dynamic source routing (DSR)[6], by using a security association between the source and destination nodes such as pair wise secret keys and end-to-end authentication [3] or design methods to detect and defend specific attacks resulting in Secure AODV (SAODV) [7], Ariadne [8], Secure Efficient Ad hoc Distance (SEAD) [9], and Authenticated Routing for Ad hoc Networks (ARAN) [10]. ON-Demand Secure Byzantine Routing (ODSBR) [16], and Highly Secure and Efficient Routing (HSER) [14] for Byzantine attacks, Rushing Attack Prevention(RAP) [15] for rushing attacks, Secure Routing Protocol [13] for impersonation and replay attacks, and Leap-Frog [17] for a single compromised node within two hops are designed to detect and defend specific attacks.

III. Improved Dynamic Key management scheme and attack detection algorithm

There are two basic security management approaches, i.e., public and secret key-based schemes. The public key-based scheme uses a pair of public/private keys and an use asymmetric algorithm such as RSA to establish session keys and authenticate nodes. In the latter scheme, a secret key is a symmetric key shared by two nodes, which is used to verify the data integrity.

Volume: 04 Issue: 06 Pages:1793-1798 (2013) ISSN : 0975-0290

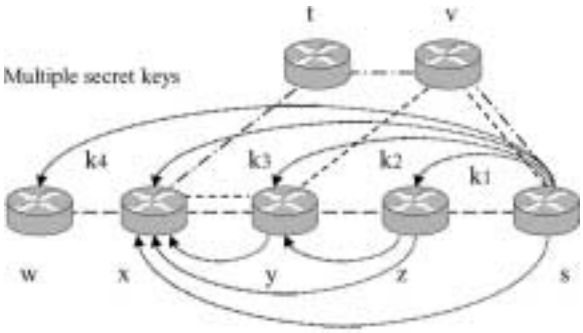

Fig.1. Multiple secret keys are shared between a source and the intermediate nodes and the destination node.

As shown in Fig.1. define a network G = (V , E) where V indicates nodes and E indicates direct wireless links between nodes. The set $N_1(x)$ define the direct neighbors of *x*.

$$N_1(x) = \{y: (x; y) \in E \text{ and } y \neq x\} \quad (1)$$

Similarly $N_n(x)$ defines hop-*n* neighbors of *x*.

$$N_n(x) = \{z : (y; z) \in E \text{ and } y \in N_{n-1}(x), z \neq x\} \quad (2)$$

Initially, a node x has a public key $K_{x,pub}$ that is distributed to $N_1(x)$ by using PKI or CA. Similarly, a node y has public key $K_{y,pub}$ distributed to $N_1(y)$.Those who hold *x*'s public key can now read the certificate and trust the binding of *y* and its public key. Based on the available certificate and key information, two hop-1 neighboring nodes can easily establish a secret key between them by using methods such as three-way handshake.

A secret key is established between the source and destination and the intermediate nodes by using public key information. Using the established multiple keys between source and intermediate nodes, each node can find out the faulty neighbors. Upon data exchange, based on the observed node behavior and attack detection results, each node updates its trustworthiness of its neighbor. Based on the local CR and maintenance procedures of public key, nodes build up self-organized PKI[13].

Let sand r denote the sender, receiver nodes respectively. The key K on message *m* where m = M + {I D_f } + S_N and M is the original message, S_N is the sequence number of the message and *h(m+k)* denotes the hash keyed algorithm with a key *k* on message *m*. At the time of route discovery, the nodes create pair wise shared keys hop by hop. The complete route request (RREQ) can be summarized as [1]

$$m+h(m + num) + E(num, K_{s,pri}) \quad (3)$$

The immediate neighbors those have the public key are able to verify the signature and decrypt the key in the message. The destination zsends back a route reply (RREP) in a similar format

$$m_p + h(m_p+k_1) + E(E(k_1,K_{s,pub}),K_{z,pri}) \quad (4)$$

where $m_p$stands for the message used in RREP. By decrypting the message and comparing the key, *s* can authenticate *z* and distribute a shared key to *z*.

By checking the acknowledgement message back from *y* via *z*, *s* can find out all of its hop-2 neighbors $N_2(s)$. Therefore, *s* can send a message to $r \in N_2(s)$ via $z \in N_1(s)$ in the following format:

$$m_2 + h(m_2 + k_1),\ k_1 =: \text{shared key between } s \text{ and } y \quad (5)$$

where

$$m_2 = m + h(m + k_2) + E\ (E(k_2,K_{r,pub}),K_{s,pri})$$
$$\text{for } r \in N_2(s) \quad (6)$$

In the above key distribution process, the same message *m* has been sent to the destination multiple times and protected by different secret keys at each time. To utilize the message redundancy, the implementation is simple: each node is required to receive multiple copies of the same route discovery message before sending back an acknowledgement. Receiving multiple copies incurs overhead to the route discovery process. This can be optimized by considering the trustworthiness of the nodes.

Once the source and destination are associated with the security agents, the source simply uses the shared key to protect the data packets. The basic step to detect a compromised node is to compare the different copies of the same message, the node has received. Nodes along the route can be found by verifying the aggregated node IDs that are attached to the message. Hence, the data is protected from passive attacks and also, the misbehaving nodes can be filtered out.

IV. Proposed Routing Algorithm

Encryption and decryption of data at each node incurs delay in data delivery and also affect the packet delivery. Trust model can be maintained , to avoid hashing at each node. Assume *x* has received a message m_t at time *t* with a total number of attempted transmissions m_a and total number of successful transmissions m_s. The trust of node *n* at node *x* can be calculated as

$$T_x(n_1) = \frac{m_s + \varepsilon m_s}{m_a + \varepsilon m_a} \quad (7)$$

where $0 < \varepsilon < 1$ is a weighing factor that represents the successful transmissions.

A statistical model similar to the model used for link quality measurement in [11] is used to optimize the QoS. This model not only evaluates the trustworthiness but also reflects the link quality. Using a moving average model,

$$T_x(n; j+1) = \alpha T_x(n;j) + (1-\alpha)T_x(n;j)$$

Volume: 04 Issue: 06 Pages:1793-1798 (2013) ISSN : 0975-0290

for n $\in N_1(x)$ (8)

Where $0 < \alpha < 1$ is a weighting factor used to tradeoff between measured value and estimated value.

The working of routing mechanism as

1. When there is a need to send data, the source node initiates RREQ which is equipped with the security information as outlined in Section II, using (6).
2. Once the intermediate node receives the RREQ, it calculates the TQI using (8). The trustworthiness of the neighbor is verified and the decision on the encryption is made.
3. At the destination, instead of waiting for multiple RREQs to reach, as proposed in [1], the destination node verifies the security information and replies to the route accordingly.
4. Once the route is established, the data is transferred by encrypting using shared keys. As the time passes by, based on the trustworthiness of the intermediate nodes in the route, the encryption is reduced.
5. Other route maintenance activities like RERR are followed as in AODV[8].

V. Simulation Results

In this section, an NS-2 simulator is used to investigate the performances of OSRWQOS and to make a comparative study with SRAC and AODV using performance measures. The simulation environment is as follows.

Simulator	NS-2
Network Area	1000x1000 m^2
Network Density	200
Number of Attackers	4 - 20
Attacks	Byzantine attack
Routing Protocols	AODV, SRAC, OSRWQOS
Performance parameters	Overhead, Packet delivery, End-to-End delay, Throughput

Table 1: Simulation Environment

The performance metrics are defined as follows.

1) *Total throughput*: The total number of data packets that have been received at time *t* by a destination node.

2) *Total overhead*: The total number of routing (control) packets that have been transmitted at time *t* by the nodes in the network.

3) *Packet latency*: The time elapsed since a data packet is transmitted to the time when it is received at the destination.

4) *Packet delivery ratio (PDR)*: The ratio of the total number of data packets successfully delivered to the destination to the total number of data packets sent out by asource node.

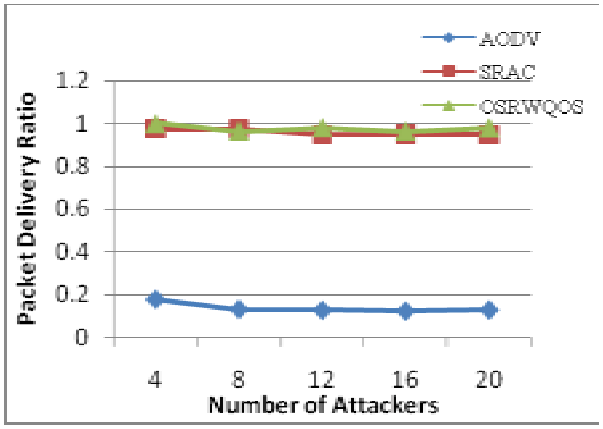

Fig.2. Packet Delivery Ratio vs Number of attackers

It can be observed from Fig.2. that OSRWQOS achieves similar packet delivery to AODV. This is because of the reduction in delay at each node and avoidance of multiple copies of data.

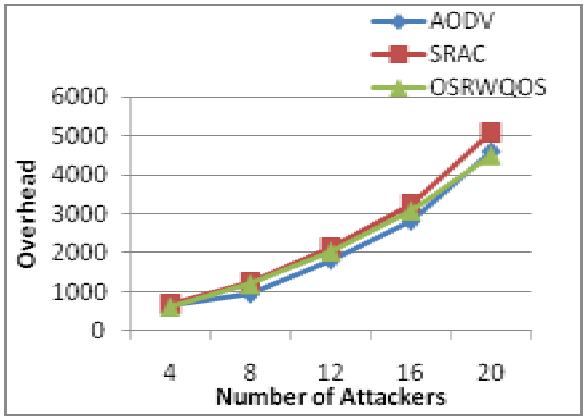

Fig.3.Overhead vs Number of attackers

It can be observed from Fig.3. The overhead incurred by OSRWQOS is much less when compared to SRAC and is close to that of AODV.

Volume: 04 Issue: 06 Pages:1793-1798 (2013) ISSN : 0975-0290

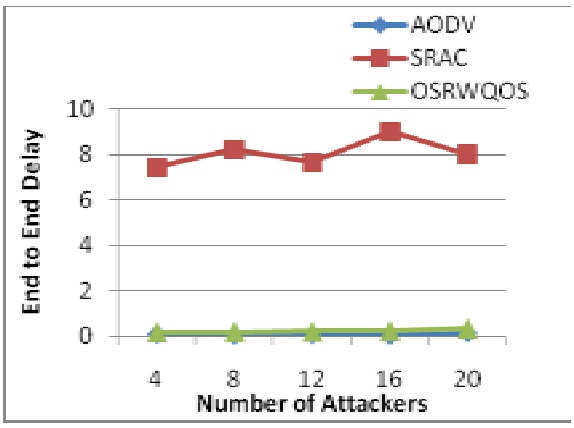

Fig.4. End-to-End delay vs Number of attackers

From Fig.4,as the delay at each node caused by encryption and verifications are avoided, OSRWQOS achieves better End-to-End delay and in-turn assures better packet delivery as AODV.

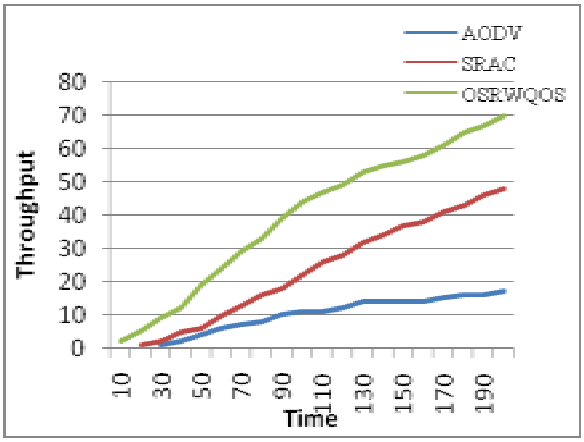

Fig.5. Throughput vs Simulation Time

It can be observed from Fig.5. that OSRWQOS out performs SRAC and AODV are with increase in time it guarantees consistently improved throughput.

VI. Conclusion

This paper has improved SRAC[1] in terms of Quality of Service achieving similar security, Optimal solution (OSRWQOS), by improving trustworthiness and avoiding delays at each intermediate node, has been framed. The simulation results that have demonstrated the effectiveness of the proposed mechanism and superiority over SRAC. OSRWQOS achieved 84% more packet delivery than SRAC and 2% nearer to AODV. Because of reduction in delays at intermediate nodes, OSRWQOS was able to deduct average End-to-End delay by 96% compared to SRAC and was 32% more to AODV. The overhead incurred by OSRWQOS is 4% more than AODV and 15% lesser than SRAC. The proposed attack detection and routing algorithm can be easily integrated to existing routing protocols such as AODV and DSR.

Use of the proposed method causes and computational burden to loose QoS in secure routing protocols and hence needs improved by implementing better trust repository and avoiding encryption and decryption at every intermediate node.

References:

[1]. Ming Yu, MengchuZhou,"A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 58, NO. 1, JANUARY 2009

[2]. C. Zhang, M. C. Zhou, and M. Yu, "Ad hoc network routing and security: A review," *Int. J. Commun. Syst.*, vol. 20, no. 8, pp. 909–925, Aug. 2007.

[3]. S. Kannan, T. Maragatham, S. Karthik and V.P. Arunachalam; A Study of Attacks, Attack Detection and Prevention Methods in Proactive and Reactive Routing Protocols; International Business Management, 2011.

[4]. J. Mirkovic and P. Reiher, A Taxonomy of DDoS Attack and DDoS Defense Mechanisms, ACM Sigcomm Computer Communications Review, Vol. 34, No. 2, Apr 2004.

[5]. XianjunGeng and Andrew B. Whinston; Defeating Distributed Denial of Service Attacks; February, 2000

[6]. D. B. Johnson, D. A. Maltz, and J. Broch, "DSR: The dynamic source routing protocol for multihop wireless ad hoc networks," in *Ad Hoc Networking*, C. E. Perkins, Ed. Reading, MA: Addison-Wesley, 2001, ch. 5, pp. 139–172.

[7]. M. G. Zapata and N. Asokan, "Securing ad hoc routing protocols," in *Proc. ACM WiSe*, Atlanta, GA, Sep. 28, 2002, pp. 1–10.

[8]. Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," in *Proc. 8th ACM Int. Conf. Mobile Comput. Netw.*, Sep. 2002, pp. 12–23.

[9]. Y.-C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in *Proc. 4th IEEE Workshop Mobile Comput. Syst. Appl.*, Jun. 2002, pp. 3–13.

Volume: 04 Issue: 06 Pages:1793-1798 (2013) ISSN : 0975-0290

[10]. K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "Authenticated routing for ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 3, pp. 598–610, Mar. 2005.

[11]. W. Liu, W. Lou, and Y. Fang, "An efficient quality of service routing algorithm for delay-sensitive applications," *Comput.Netw.*, vol. 47, no. 1, pp. 87–104, Jan. 2005.

[12]. Hwee-Xian Tan and Winston K. G. Seah; Framework for Statistical Filtering Against DDOS Attacks in MANETs; Proceedings of the Second IEEE International Conference on Embedded Software and Systems; 2005.

[13]. P. Papadimitratos and Z. Haas, "Secure routing for mobile ad hoc networks," in *Proc. SCS Commun.Netw.Distrib. Syst. Model. Simul. Conf.*, Jan. 2002, pp. 27–31.

[14]. Z. Wang, L. Liu, and M. C. Zhou, "Space and network diversity combination for masked node collision resolution in wireless ad hoc network," *IEEE Trans. Wireless Commun.*, vol. 6, no. 2, pp. 478–485, Feb. 2007.

[15]. Y.-C. Hu, A. Perrig, and D. B. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols," in *Proc. ACM WiSe*, Sep. 2003, pp. 30–40.

[16]. B. Awerbuch, R. Curtmola, D. Holmer, and C. Nita-Rotaru, *ODSBR: An On-Demand Secure Byzantine Routing Protocol*, Oct. 15, 2003, JHU CS Tech. Rep., Ver. 1.

[17]. M. T. Goodrich, "Leap-frog packet linking and diverse key distributions for improved integrity in network broadcasts," in *Proc. IEEE Symp. Security Privacy*, 2005, pp. 196–207.

Authors Biography

K.Sreenivasulu presently working as professor & HOD CSE in Madina Engineering College Kadapa.AP He is currently pursuing Ph.D from JNTUK He received B.E in Computer science from Bangalore University. He received his M.Tech in Computer Science from JNT University .He is having more than 13 years of experience in teaching. He has guided several graduate & post graduate students in their Academic projects.

Dr. E. V. Prasad received B.E. degree in ECE from S.V. University, Tirupati, A.P., India, in 1975. He obtained M.E. in Control Systems from Madras University, Madras, India, In 1978. He received his Ph.D. degree in Computer Science and Engineering, from University of Roorkee (IIT Roorkee) in 1990. He is having 34 years of teaching experience. He received best teacher award from Government of Andhra Pradesh, for the year 2008. During his teaching profession, he worked at different capacities such as Principal, Director I.S.T and Registrar JNTUK. Currently he is working as Rector J.N.T. University Kakinada, Kakinada, India..He is co-authored for many text books. He is life member of ISTE, IE(I), CSI, and IEEE. He has more than 96 research publications in proceedings of National, International Conferences, National and International Journals

Dr.A.Subramanyam received his Ph.D. degree in Computer Science and Engineering from JNTU College of engineering, Anantapur. He has obtained his B.E.(ECE) from University of Madras. M.Tech.(CSE) from Visweswaraiah Technological University. He is having 19 years experience in teaching. He is currently working as professor & HOD in the Department of Computer Science Engineering of Annamacharya Institute of Technology & Sciences, Rajampet, KADAPA Dist. A.P.. He has presented and published number of papers in international and national and conferences and number of technical paper in international and national journals. He is guiding few Ph.D.s. His research areas of interest are parallel processing, image processing, network security and data ware housing, mobile computing