ISSN : 2231-0711

Jaspreet Kaur et al | IJCSET(www.ijcset.net) | July 2015 | Vol 5, Issue 7,219-223

An Energy Efficient, Secure and Trust Aware Routing Protocol in MANET

Jaspreet Kaur
Department of Computer Science and Engineering
PEC University of Technology
Chandigarh, India

Dr. Sandeep Harit
Department of Computer Science and Engineering
PEC University of Technology
Chandigarh, India

Abstract— Mobile ad hoc network (MANET) security has become the primary focus of research efforts in ad hoc communication environment. Dynamic nature of MANET results into unique and considerable difficulties of providing security. Many security schemes have been proposed to protect the communication in an ad hoc network. This paper includes detailed analysis on secured extension to AODV i.e Secure ad hoc on demand distance vector protocol (SAODV) and TSAODV . In this paper, we provide an overview of various attributes, dataset, key parameters and methods adopted for vulnerability analysis of Manet protocols to identify unresolved threats to the algorithm, such as malicious node misbehavior, resources depletion, resources consumption, Denial of service and replay attacks. A vulnerability analysis of security extensions to AODV protocol and results concluded by various researchers are also included. This paper includes a proposed methodology to make SAODV protocol more robust, reliable and energy efficient protocol to overhear cryptography and long term communication.

Keywords— SAODV, encryption, trust, energy

I. INTRODUCTION

Due to rising trend in mobile ad hoc networks (MANETs) security flaws are also increasing very rapidly. There are many security protocols have been designed to make Manet communication secure, reliable and robust. An on demand reactive protocol AODV is used for communication in MANET. But, It has many security glitches i.e attacker can drop, modify and forward routing control messages, replying with forged messages etc. SAODV can fight various types of vulnerabilities of AODV i.e Route Disruption, Route invasion, Node isolation and Resource depletion. Resource depletion is one of the serious issue as battery power is critical to save. Denial of service and bandwidth allocation in the presence of scarce resources is current area of research of many researchers [3]. Dos may flood the network with excessive RREQ's or RERR to use resources and drain the battery power of nodes [1]. SAODV takes security into account while transmitting routing messages and assures to give minimal routing exposure [8] .

According to various security solutions embedded into AODV each proposed Secure AODV have its own definition of detection and prevention of security attacks. Secure Ad hoc on demand distance vector protocol (SAODV) uses hybrid cryptography and provides security features such as integrity, authentication and non repudiation of routing data. These security solutions are based on two assumptions Key management scheme and Secure IP public key binding. SAODV provides security in route discovery and a feature of import authorization, which makes a node authorize to update routing information when destination node receives the information. SAODV has two important features one is Digital signatures to authenticate the non-mutable fields of the messages and other is Hash chains to secure the mutable hop count field of the message. Digital signatures are used to sign Route Request (RREQ) and Route Reply (RREP) packet which provides integrity. Digital signature helps to verify the originator of message. Hop count field in RREQ and RREP is mutable and needs to changed by each node when there is active communication in network. So, here is issue to allow intermediate nodes to participate in communication. To address this two approaches called respectively Single Extension and Double Signature Extension are used. Packets generated via these extensions allow each node to verify the validity of packets. If verification results to fail node discards packet information. SAODV uses online key management system to make its assumptions true.

SAODV is still vulnerable to Sleep Deprivation attack , Rushing and wormhole attack. Sleep Deprivation attack and Wormhole attack aims to drain off limited resources in mobile ad hoc networks. In sleep deprivation malicious node targets the victim node by flooding unnecessary RREQ, RRER and RREP packets. As a result, victim node refrains from participating in the network communication. Malicious node may send route request (RREQ) to destination address that do not exists in network, or sends too many requests without any time interval. In *Rushing attack* attacker exploits route discovery phase in ad hoc networks. Malicious node broadcasts a rushed RREQs which will reach other nodes before legitimate RREQs, causing the legitimate RREQs to be discarded when they arrive later.

Wormhole attack [2] comes under category of resource depletion attacks in the network. Attacker replays data and control packets through high speed wired and wireless link controlled by itself. Collaborating attacker nodes make a high speed tunnel on the dominating positions in the network and thereby makes control over the whole network. Main aim is to draw all traffic from network which hinders the availability to other nodes. Main issue is of detection of wormhole in the major network scenarios.

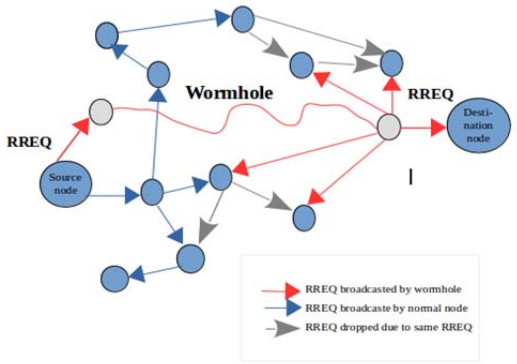

Figure 1. In band Wormhole attack

SAODV does not prevents a network from internal attacks. It does not take into account if a fair node is compromised at later time. Internal attacks may occur at later stage when a node becomes malicious or acts selfish to prevent its battery power and tries to consume other nodes battery. There are certain trust based secure AODV schemes present to make AODV secure from internal attacks. Trust evaluation system can improve network throughput as well as effectively detect malicious behavior in ad hoc networks. Network Performance will automatically improve when sender node skips malicious nodes based on trust values. However, Trust can be interpreted as reputation, trusting opinion and probability.

Security always comes with a high cost of energy. The drain on the battery sets the energy expenses of the device. "The consumption of running cryptographic algorithms when the batteries are low charged is around 16% higher than when they are full"[18]. In Manet nodes work on battery power and it is not possible to recharge its battery during an active communication. Cryptography always puts various challenges in term of energy draining [10]. Also, Researchers explained security and power consumption challenges in ad-hoc networks [17]. So, there should be a scheme that can make Manet communication secure from external, internal attacks by using least battery power. This paper provides an insight into this solution.

The structure of the paper is organized as follows: next Section describes related work carried out in this domain. In Section 3, we explain a already existed protocol Trust aware secure on demand ad hoc protocol (TSAODV) and its limitations. Section 4 gives our proposed methodology to reduce trade off between security and power consumption, which is followed by next section which emphasizes on conclusion and future scope of concerned work.

II. RELATED WORK

Many security improvements have been proposed to make SAODV a robust protocol to communicate in Manet. Floriano De Rango[5] contributed two kinds of approaches applied to well known routing protocol SAODV. A preventive approach to improve network performance is proposed. For this extension of SAODV to offer Intrusion Detection mechanism(IDM) and trust based mechanism(TBM) to promote collaboration of the cooperating node and penalize the selfish nodes are proposed. A new protocol SAODV-SDDO is being proposed and evaluated. This protocol provides solution against selfish behavior of nodes and penalized the actions of selfish nodes. Also actions of collaborating nodes are rewarded. This work is based upon Selfish nodes detection throughout Credit Management and Trust based Mechanism.

In [6] vulnerability analysis of AODV and Secure AODV (SAODV) routing protocols against routing attacks have been done. However, SAODV has vulnerabilities of its own that allow replay attacks to succeed. Libzcrypt and Openssl encryption libraries are used for digital signature and creation and hash chain generation. Therefore, author proposed a new security scheme Robust SAODV (R-SAODV), which incorporates temporal time stamping of SAODV extensions. Various attack simulations have been done in order to make solutions robust. This study presents a clear comparison of AODV, SAODV and R-SAODV s sensitivity towards replay attacks. R-SAODV with the help of temporal time stamping in SAODV extension message fully combats replay attack.

Andrea Lupia [4] has offered a new security solution considering energy conservation concept in MANET. This study comprises of energetic analysis on SAODV. Also trust management system is introduced to protect against black hole and gray hole attacks, in addition to already existed cryptographic solutions. Study has adopted a framework of trust modeling and evaluation [14] and Energy Consumption model for performance analysis [15]. Results of energy consumption of cryptographic algorithms have been used [16] . Author has done a comparative analysis of SAODV and Trusted SAODV.

III. TRUST AWARE SECURE AD HOC ON DEMAND DISTANCE VECTOR PROTOCOL (TSAODV)

We have included information Theoretic Framework and model [11] in our studies..Trust is measure of uncertainty with its value represented by entropy. There are four axioms that address basic understanding of trust and rules for trust propagation.

- Entropy based trust value :- Information Theory states that entropy is a nature measure for uncertainty. Entropy based trust values are defined as :-

$$T\{\text{Subject : agent,action}\} = \begin{cases} 1 - H(p), & \text{for } 0.5 < p <= 1 \\ H(p) - 1, & \text{for } 0 < p < 0.5 \end{cases}$$

Subject T{subject : agent,action} denotes the trust value of the relationship {subject : agent,action} and P{subject : agent,action} denotes probability that the agent will perform the action in the subject's point of view. Probability is opinion of subject only. Trust value is a continuous real number lies in interval [-1,1]. Trust value is negative for $0<p<0.5$ and positive for $0.5 < p <= 1$ [11].

There are four axioms driven for core understanding of trust based model and recommendation model in which Axiom 1 states meaning of trust. Axiom 2 states rule for concatenation trust propagation. Axiom 3 describes the rule for multipath trust propagation. Axiom 4 addresses the correlation of recommendations. We have used axiom 1 for our proposed work states that Uncertainty is a measure of trust. [11]

The multi-hop recommendation based trust management scheme (TRUISM) [19] uses a probabilistic approach for calculating trust from multiple contradictory recommendations. Trust management scheme is introduced in SAODV that already provides encryption methods to authenticate individual nodes to provide network from external attacks. A unique proposal regarding trust management scheme along with cryptography is given in [4]. A trust table is introduced in network, each node is assigned with a trust values and a value is calculated.

- Route discovery is done as same as the SAODV does. Trustworthiness metric is used to add next hop of a route.
- According to Recommendation model, two new packets TRREQ, TRREP are used.
- On the basis of recommendations and interactions made by nodes communication is continued.
- Energy model has been used to calculate energy due to more packet overhead and algorithm complexity.

This protocol gives a robust solution on maliciously packet dropping because it excludes malicious nodes from its route. In terms of security it is most reliable protocol that can prevent from both external and internal attacks but if energy is not constrained. Use of promiscuous mode, to receive all the data packets in its wireless range consumes more energy. Thats is the biggest limitation.

IV. PROPOSED SOLUTION

The various authors analyzed the energy consumption of various routing protocols in DTNs, evaluating the impact on the performance of the protocols [15]. It is proved that "Broadcast Flooding" in Manets is an expensive operation. [9] It is being experimentally proved SAODV has higher over load due to asymmetric cryptography [17], as it needs considerable processing time to verify signatures and hashes at each node. [7] The work done in [16] the authors proposed an algorithm to achieve an energy efficient, secure and stable routing over MANETs. In our proposed solution, an energy efficient algorithm is introduced to trusted SAODV along to make it an energy efficient protocol. To conduct this study we have used results of recommendation model [20] , Energy model [9] and ALMEL-AODV[13] for analysis of AODV variant energy efficient solution in MANET scenarios. Proposed algorithm states that:-

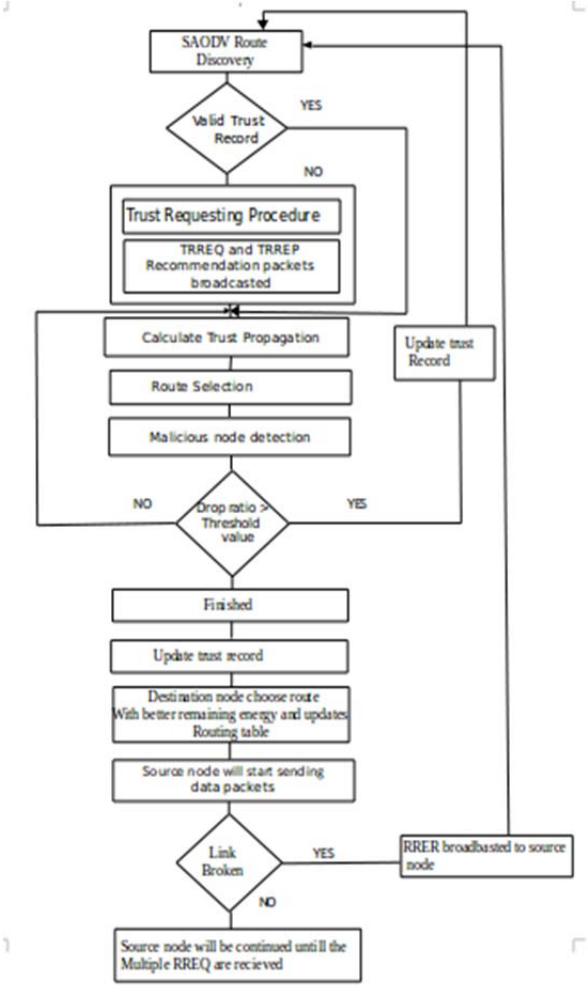

Figure 2. Flowchart of Proposed Solution

Route Requests are managed by SAODV by Route Discovery Algorithm which takes into account RREQ with fresh sequence numbers and discards older ones. This updates routing table adding the new next hop of route. Node will choose next hop of route on the basis of two metrics that is Trust worthiness and Recommendation model. We have adopted framework of trust methodology and evaluation[11], which implements the trust management capability to SAODV protocol.

Based on recommendation model two new packet typologies Trust Recommendation Request (TRREQ) and Trust Recommendation Reply (TRREQ) [4] are used. TRREQ comprises of request originator and a list of requests about agents to check whether they are reliable or not. TRREP comprises of the originator, the recommender, who generates reply and a list of couples <agent, trust values>. Signature extension is added to make it cryptographically secure packets.

Maximum Remaining Energy :- Sum of Remaining energy of nodes in a route for route selection can be used as an important metric to choose next hop. This will help for longer transmission and reliable communication [12]. However, to reduce complexity of this algorithm only non-malicious nodes will be checked for maximum remaining energy.

Detailed Steps of algorithm are explained below :-

- Source node performs on-demand routing to find possible routes to Destination nodes. 'S' puts obtained recommended observations in the recommendation buffer, and constructs a trust propagation graph based on its own trust record and the recommendation buffer.
- Based on trust graph, nodes calculates trust values for the nodes. Trust table is introduced in the network, which contains agent, parameters that allows computing the trust values and updating it when needed. Recommendations, direct observations, agent information is updated periodically. If a forwarding packet has trust value less than 0, it is included in blacklist and removed for all routes stored. [11] If a route selected for communication has a single blacklisted node as next hop, route is invalidated. Then, new route discovery process is started.
- When a node is said to be trusted by source node, then it will check for remaining energy of neighbor nodes. If remaining energy of node is near to zero, node is disallowed from broadcasting RREQ packets. Otherwise it adds the energy information of node to accumulated energy field in the RREQ.
- When trusted destination node receives first route request packet, the node will calculate and update accumulated energy field on the destination node route table. It uses a method to calculate remaining energy on the basis of data packets sent or received.
- If a route with trust and better energy sum recieved the destination node will enter new information and alternate path is added to the routing table. After that, destination node unicast RREQ to source node using reverse link.
- If a link is broken, route error packet will be sent to source node and source node will select alternate route from its route table otherwise does route discovery. Then whole algorithm is repeated.

This method provides an better insight to choose only those non- malicious nodes which are remained with good battery power to maintain a longer and reliable transmission. Only Energy efficiency can also be included into trusted nodes [14], but adding the concept of cryptography here, there can be prevention of external attacks

IV. CONCLUSION

Security overloads the network with cryptographic solutions. As a result, network performance is degraded and each time power saving is critical. Therefore, there should be a solution that can prevent nodes from draining battery, and that can provide load balancing between nodes. However, trust management and cryptographic solutions merging together under an energy aware perspective can provide a robust solution to secure routing protocols. Network simulator 2.35 provides a vision to real-time network scenarios, attack simulations and security algorithms. To analyze protocol efficiency various approaches are used by choosing different attributes. It is observed that security can be improved if nodes make intelligent choices of non-malicious nodes and if contextual information is known in the form of routing tables. Battery capacity can be fully utilized if long term transmission is negotiated with powerful nodes only. Robust security and performance must be taken into same path so that Manet features can build a better performance in real time scenarios, mobile devices and military environment.

REFERENCES

1. Peng Ning, Kun Sun, “How to misuse AODV: a case study of insider attacks against mobile ad-hoc routing protocols”, Science Direct, 2004
2. Todd.R. ANDEL, “Surveying Security Analysis Techniques in Manet Routing Protocols”, VOLUME 9, NO. 4, 2007
3. Jan von Mulert, Ian Welch , Winston K.G. Seah, “Security threats and solutions in MANET: A case study using AODV and SAODV”, Journal of Network and Computer Applications, Elsevier, 2012, pp. 1249-125
4. Andrea Lupia, Floriano De Rango “Evaluation of the Energy Consumption Introduced by a Trust Management Scheme on Mobile Ad-hoc Networks”, Journal of Networks , vol. 10, no. 4, April 2015
5. Floriano De Rango, “Improving SAODV Protocol with Trust levels management, IDM and Incentive Cooperation in MANET ”, Wireless Telecommunications Symposium, IEEE , 2009
6. F Maan, Abbas, Y. Abbas , N. Mazhar, “Vulnerability Assessment of AODV and SAODV Routing Protocols against Network Routing Attacks an Performance Comparisons ” , Conference on Wireless Advanced (WiAd) , IEEE, 2011, pp. 36-41, June 2011
7. Manoj Yadav, Sachin Kumar Gupta, R. K. Saket, “Experimental Security Analysis for SAODV vs SZRP in Ad-hoc Networks, ” Sixth International Conference on Computational Intelligence and Communication Networks, IEEE, pp. 819-823, Nov. 2014
8. Ayman A. Hanafy, Sherif H. Noureldin, Marianne A. Azer, “ Immunizing the SAODV Protocol Against Routing Information Disclosure, 6th International Conference on Internet Technology and Secured Transactions, pp. 330 – 334, Dec 2011
9. Laura Marie Feeneyl, “An Energy Consumption Model for Performance Analysis of Routing Protocols for Mobile Ad Hoc Networks ”, Computer and Network Architectures Laboratory, Mobile Networks and Applications, vol 6, 239–249, 2001
10. N. R. Potlapally, S. Ravi, A. Raghunathan, and N. K. Jha, “A study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols,” IEEE Transactions on Mobile Computing, vol. 5, no. 2, February 2006.
11. Yan Lindsay Sun, Wei Yu , Zhu Han, K. J. Ray Liu, “Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks”, IEEE Journal on Selected Areas in Communication, vol. 24, no. 2, Feburary 2006
12. Shival Chadda, Mritunjay Kumar Rai, “A Review of Energy Efficient and Secure Routing Protocols for Mobile Ad-hoc Network”, International Conference on Computing, Communication and Information Technology , 27 - 29 June, 2012
13. Tai Hieng Tie , Chong Eng Tan , Sei Ping Lau, “Alternate Link Maximum Energy Level Ad Hoc Distance Vector Scheme for Energy Efficient Ad Hoc Networks Routing ”, International Conference on Computer and Communication Engineering, May 2010
14. M. Pushpalatha, Revathi Venkataraman, and T. Ramarao, “Trust Based Energy Aware Reliable Reactive Protocol in Mobile Ad Hoc Networks”, World Academy of Science, Engineering and Technology , Vol:3, 2009
15. A. Socievole, and S. Marano, “Evaluating the Impact of Energy Consumption on Routing Performance in Delay Tolerant Networks,” IEEE Wireless Communications and Mobile Computing Conference, pp. 481-486, August 2012.
16. S. Taneja, and A. Kush, “Energy Efficient, Secure and Stable Routing Protocol for MANET,” GS. Taneja, and A. Kush, “Energy

Efficient, Secure and Stable Routing Protocol for MANET," Global Journal of Compuer Science and Technology, 2012

17. G. Sharma, and M. Fatima, "Security & Power Consumption Challenges in MANET: A Review," International Journal of Advances in Engineering & Technology, vol. 6, no. 3, pp.1199-1204, July 2013
18. H.Rifà-Pous, and J. Herrera-Joancomartì, "Computational and Energy Costs of Cryptographic Algorithms on Handheld Devices," Future Internet, vol. 3, pp. 31-48, February 2011
19. K. Z. Bijon, M. M. Haque, and R. Hasan, "A Trust Based Information Sharing Model (TRUISM) in MANET in the Presence of Uncertainty," 12th Annual InternationalConference on Privacy, Security and Trust, IEEE, 2014.
20. F. Zhang, "Preventing Recommendation Attack in Trust- Based Recommender Systems," Journal of Computer Science and Technology, vol. 26, no. 5, pp. 823-828, September 2011.