International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 6 | ISSN : 2456-3307

Designing of Authentication Based Security in MANETs

Yumana Zaidi[1], Naveen Kumar[2], Parul Saharavat[3]
[1]M.Tech Scholer J.P.I.E.T, Meerut, Uttar Pradesh, India
[2]Department of computer science J.P.I.E.T, Meerut, Uttar Pradesh, India
[3]Department of computer science D.N. Polytechnique, Meerut, Uttar Pradesh, India

ABSTRACT

Current ad hoc routing protocols assume the networks to be benevolent and cannot cope with misbehavior of nodes. The misbehavior may be due to node being malicious or selfish to save the battery power. Thus, this work is of significant importance because now-a-days, new cryptographic schemes, such as threshold cryptography, are used to build a highly secure key management service that forms the core of security framework presented in this work. The CONFIDANT (Cooperation Of Nodes: Fairness In Dynamic Ad-hoc Network) on DSR (Dynamic Source Routing Protocol) is simulated in order to evaluate how the network performance changes as dynamic feedback mechanisms are introduced in an ad hoc network to control the node misbehavior. The above results have been used to design a trust based routing protocol that uses reputation data to provide dynamic feedback.

Keywords : MANET, DSR, Key Management Service, Good Throughput, Evil Drop Rate.

I. INTRODUCTION

Mobile Ad Hoc Network (MANET) is a collection of wireless mobile nodes that dynamically communicate amongst themselves without the use of any existing infrastructure and centralized/decentralized administration. The mobile nodes must cooperate at the routing level in order to forward packets to from source to the destination. Current ad hoc routing protocols such as Dynamic Source Routing (DSR) [1] assumes the network is benign and cannot cope with misbehavior, i.e., a misbehaved node may drop packet silently to save battery power, etc.

This paper investigates dynamic feedback mechanisms as a security solution for MANETs, implements CONFIDANT protocol using ns2 as simulation environment, and evaluates the performance of CONFIDANT fortified DSR in the MANET where misbehaved nodes are present. The simulation results are analyzed and compared with that of standard DSR.

We propose a reputation-based trust management scheme to detect misbehaving nodes and to exclude them from the network. This is done by monitoring the neighbors, which results in a direct trust value, and by asking others for reputation. Direct trust and reputation together form total trust, which then is used for routing decisions. To be able to control routing decisions from source to destination, a source routing protocol is needed. Therefore, we considered the DSR protocol and extended it on our trust management. Finally, we conclude with the future scope.

II. RELATED WORK

Computer networks were originally developed to operate by connecting computers together with wires and transmitting data over these wires. Network sizes

and occurrences increased creating a requirement for inter-network communication. This led to the development of the Internet and its suite of protocols. The use of the Internet and its applications became ubiquitous. A need for providing network access to entities while not physically attached to the wired network arose. To enable this wireless networking was developed, providing devices with methods to connect to a wired network using radio wave technologies through wireless access points. Simultaneously, telephone networks were undergoing a similar transformation. Cellular network technologies [4] were developed to allow mobile phones to connect via base stations and communicate in a circuit switched environment. The area of mobile ad-hoc networking deals with devices equipped to perform wireless communication and networking, but without any existing infrastructure such as base stations or access points. Wireless devices form a network as they become aware of each other's presence. They communicate directly with devices inside their radio range in a peer-to-peer nature and to communicate with a device outside their range, they can use an intermediate device or devices within their radio range to relay or forward communications to the device outside their range.

III. MAJOR SECURITY ATTACKS ON MANETS

Current ad hoc routing protocols are basically exposed to following types of attacks:

- Eavesdropping
- Impersonation
- Modification
- Fabrication
- Wormhole Attack
- Lack of cooperation
- Denial of Service (DoS)
- Routing Disruption attacks

IV. ALGORITHM

Distribution of trust in our key management service is accomplished using threshold cryptography. An (n, t + 1) threshold cryptography scheme allows n parties to share the ability to perform a cryptographic operation (e.g., creating a digital signature), so that any t + 1 parties can perform this operation jointly, whereas it is infeasible for at most t parties to do so, even by collusion. In our case, the n servers of the key management service share the ability to sign certificates. For the service to tolerate t-compromised servers, we employ an (n, t+1) threshold cryptography scheme and divide the private key k of the service into n shares ($s_1, s_2, \ldots, s_n$), assigning one share to each server. We call ($s_1, s_2, \ldots, s_n$) an (n, t + 1) sharing of k. Figure 3-2 illustrates how the service is configured. For the service to sign a certificate, each server generates a partial signature for the certificate using its private key share and submits the partial signature to a combiner. With t + 1 correct partial signatures, the combiner is able to compute the signature for the certificate. However, compromised servers (there are at most t of them) cannot generate correctly signed certificates by themselves, because they can generate at most t partial signatures. Figure 3-3 shows how servers generate a signature using a threshold signature scheme.

When applying threshold cryptography, we must defend against compromised servers. For example, a compromised server could generate an incorrect partial signature. Use of this partial signature would yield an invalid signature. Fortunately, a combiner can verify the validity of a computed signature using the service public key. In case verification fails, the combiner tries another set of t + 1 partial signatures. This process continues until the combiner constructs the correct signature from t + 1 correct partial signatures. More efficient robust combining schemes

are proposed. These schemes exploit the inherent redundancies in the partial signatures (note that any t+1 correct partial signatures contain all the information of the final signature) and use error correction codes to mask incorrect partial signatures.

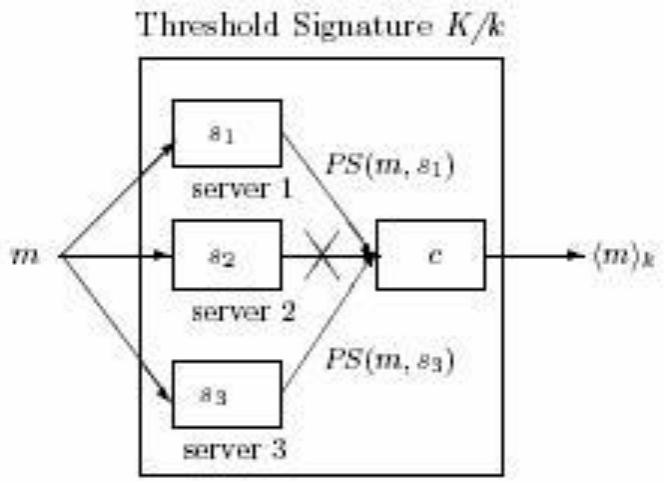

Figure 3.3. Threshold signature: given a service consisting of 3 servers.

V. EVALUATION PARAMETERS

Throughputs and Evil Drop Rate

Throughput is the most important metrics in our performance evaluation. Since the purpose of CONFIDANT is to improve the throughput for good nodes while bearing grudges to evil nodes, we evaluate the throughputs of good nodes and evil nodes separately

VI. GOOD THROUGHPUT

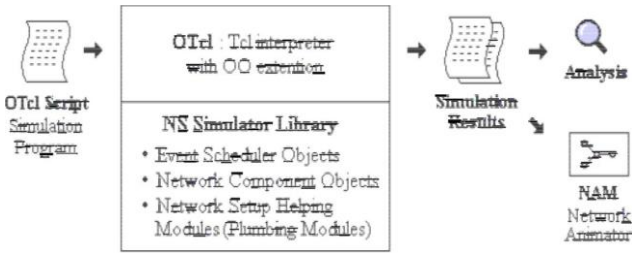

Figure 5.5. presents the good throughputs of CONFIDANT and standard DSR

Evil Throughput

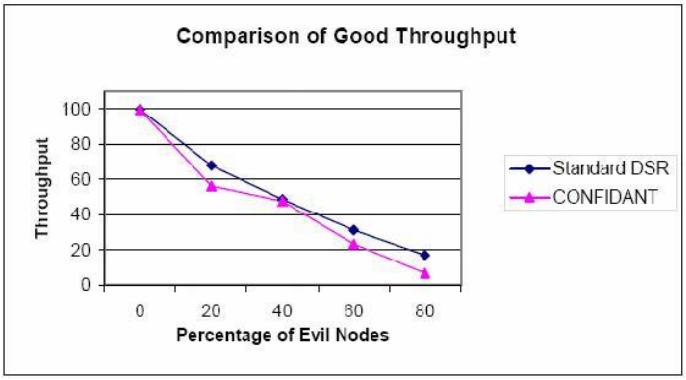

Figure 5-6. presents the evil throughputs of CONFIDANT and standard DSR.

Evil Drop Rate

The evil drop rate is the percentage of packets dropped by evil nodes in all the dropped packets. It reflects how much the evil drop contributes in overall packet drop compared to other drop reasons. Equation 5-3 is used to calculate the evil drop rate. Figure 5-8 shows the evil drop rates of CONFIDANT and standard DSR. As seen in the figure, the evil drop rate of CONFIDANT is significantly lower than that of standard DSR for all percentages of evil nodes. It is kept under 6%. This means that fewer packets are routed by evil nodes. This result fulfills the purpose of CONFIDANT that the misbehaved nodes should be avoided in forwarding packets.

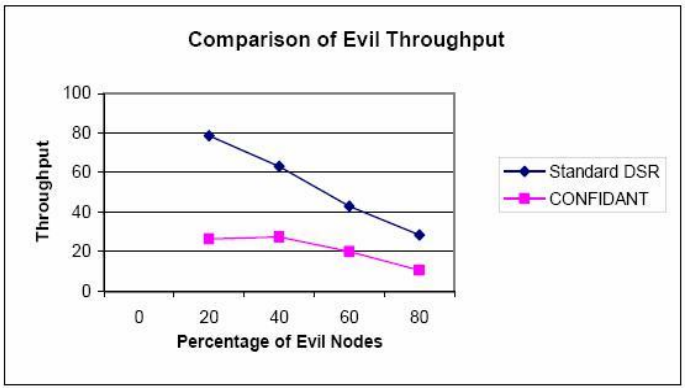

Figure 5.7. Comparison of evil throughput

Overhead

As stated earlier, CONFIDANT increases the network overhead by publishing firsthand information. It may also increase Route Request and Route Reply since it uses stricter route selection

strategy and initiate Route Discovery to find safe routes.

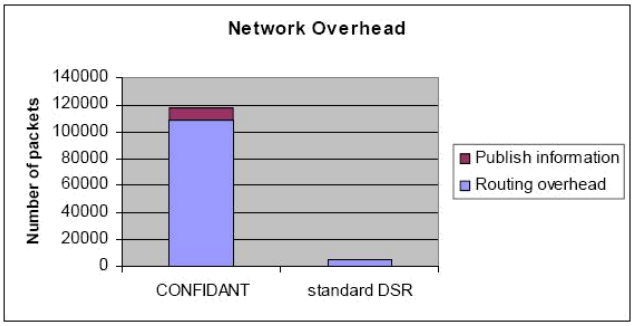

Figure 5.8. shows the network overhead of CONFIDANT and standard DSR.

VII. CONFIDANT WITH PATH RE-RANKING

An alternative route selection strategy is path re-ranking. With classic CONFIDANT, the Path manager only selects a route containing no misbehaved nodes, whereas with Path re-ranking the Path manager selects a route based on the reputation metrics of the route. In our implementation, we use a simple reputation metrics that is the average of the mean reputation values of all the nodes along the route. The advantage of Path re-ranking is that the packets will be sent out as long as there exists a route to the destination. Thus the send buffer drop rate would be decreased. However, Path re-ranking may have higher evil drop rate compared to the classic CONFIDANT since the selected route may contains misbehaved nodes.

As seen in the figures, the good throughput, evil throughput and evil drop rate of Path re-ranking lie between those of standard DSR and classic CONFIDANT. Although Path re-ranking has slightly higher good throughput than classic CONFIDANT, it is not very effective at deterring evil nodes from misbehaving because the evil throughput and the evil drop rate remain high. Thus we get the conclusion that the classic CONFIDANT can better cope with misbehavior than Path re-ranking does.

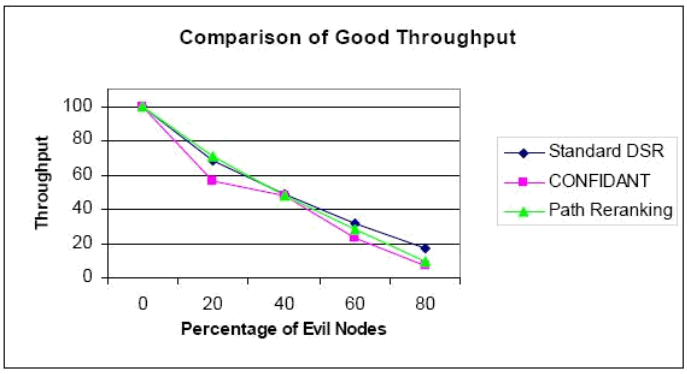

Figure 5.9. Network overhead evaluations

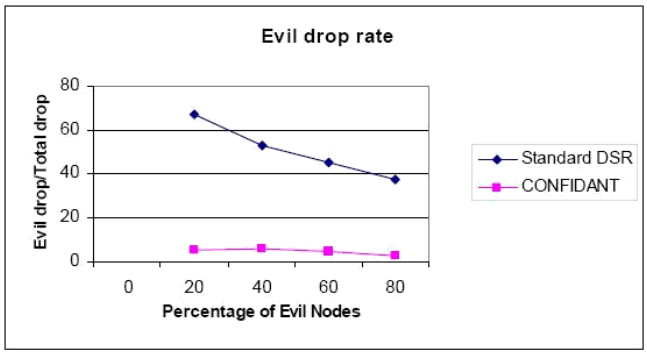

Figure 5.10. Good throughput of Path re-ranking

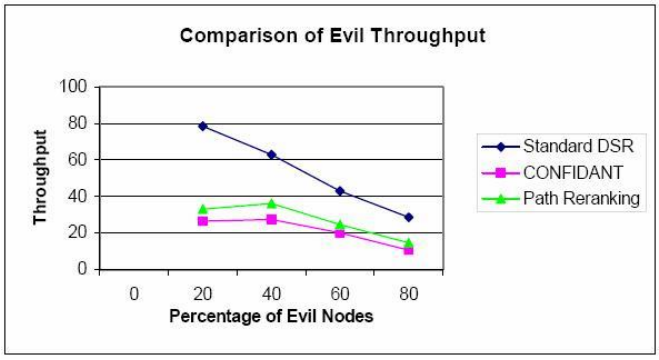

Figure 5.11. Evil drop rate of Path re-ranking

VIII. CONCLUSIONS

The presented work has carried out the sub-tasks and completed the objective as listed in chapter 4. We sincerely hope that our work will contribute in providing further research directions in the area of trust-based security. A large amount of simulations have been conducted to evaluate the performance of CONFIDANT fortified DSR. The simulation results show that CONFIDANT significantly decreases the evil throughput and evil drop rate by up to more than 50%. It proves that CONFIDANT can effectively

mitigate misbehavior in the network. However CONFIDANT does not improve the good throughput due to the large increase of send buffer drop, which is caused because there are not enough good routes in the network.

IX. REFERENCES

[1]. David B. Johnson, David A. Maltz, Josh Broch. DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks. In Ad Hoc Networking, edited by Charles E. Perkins, chapter 5, pages 139-172. Addison-Wesley, 2001.

[2]. Dellarocas C. The digitization of word-of-mouth: Promise and challenges of online feedback mechanisms. In Proceedings of Management Science 2003, Volume 49, No. 10, pages 1407–1424. INFORMS, October 2003.

[3]. Levente Buttyan and Jean-Pierre Hubaux. Stimulating cooperation in self-organizing mobile ad hoc networks. In Mobile Networks and Applications, Volume 8, Issue 5, pages 579 – 592. Kluwer Academic Publishers, 2003.

[4]. H. Armbruster. Broadcast Communications and Its Realization with Broadband ISDN. IEEE Communications Magazine, Volume 25, No. 11, pages 8-19. November 1997.

[5]. Jean-Pierre Hubaux, Levente Buttyan and Srdan Capkun. The Quest for Security in Mobile Ad hoc Networks. In Proceedings of International Symposium on Mobile Ad Hoc Networking & Computing, pages146-155. ACM Press, 2001

[6]. Y. Hu, A. Perrig, and D. Johnson. Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad Hoc Networks. Technical report TR01-384, Department of Computer Science, Rice University, 2001.

[7]. Sencun Zhu, Sanjeev Setia, Sushil Jajodia. LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks. In Proceedings of 10th ACM Conference on Computer and Communications Security (CCS '03), Washington D.C., pages 62-72. ACM Press, October, 2003.

[8]. Yih-Chun Hu, D. Johnson, A. Perrig. Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols. In Proceedings of the ACM Workshop on Wireless Security (WiSe 2003), pages 30-40. Sep. 2003.

[9]. J.R. Douceur. The Sybil attack. In Proceedings of 1st International Workshop on Peer-to-Peer Systems (IPTPS _02). Springer, March 2002.

[10]. H. Deng, W. Li, and Dharma P. Aggarwal. "Routing Security in Ad Hoc Networks. In IEEE Communications Magazine, Special Topics on Security in Telecommunication Networks, Vol. 40, No. 10, pages 70-75. October 2002.

[11]. L.M. Feeney and M. Nilsson. Investigating the energy consumption of a wireless network interface in an ad hoc networking environment. In Proceedings of IEEE Conference on Computer Communications (IEEE InfoCom), Anchorage AK, USA, Vol. 3, pages 1548–1557. April 2001.

[12]. Y. -C. Hu, D.B. Johnson, and A. Perrig. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks. In Proceedings of 4th IEEE Workshop on Mobile Computing Systems and Applications, Callicoon, NY, pages. 3-13, June 2002