International Journal of Technology and Engineering System (IJTES)
Vol 7. No.1 2015 Pp. 49-53
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976-1345

A PROBABILISTIC MISBEHAVIOR DETECTION SCHEME ON TRUST ESTABLISHMENT IN MANETS

C.VIJAYAKUMARAN[1] , T.LAKSHMANA KUMAR[2]
[1]*assistant professor* , [2]*pg scholar*
department of computer science and enginnering
valliammai engineering college
chennai, tamilnadu, india.
[1] *c_vijayakumaran@yahoo.com* , [2] *laxman2789@gmail.com*

ABSTRACT

Adversary detection in MANETs is very useful for scores of applications such as military, satellite, interplanetary and disaster rescue. Selfish antonyms and malicious behaviors represent a serious threat against routing in Mobile Ad-hoc Networks (MANETs). Due to the unique network characteristic, designing a misbehavior detection scheme in MANET is regarded as a great challenge. In this paper, an approach called iBelieve is proposed with a probabilistic misbehavior detection scheme, for secure MANET routing towards efficient trust establishment. The basic idea of iBelieve is to introduce a periodically available Trusted Authority (TA) to judge the node's behavior based on the collected routing evidences and probabilistically checking. The iBelieve is modeled as an Inspection Game and game theoretical analysis is used for demonstration purpose by setting an appropriate investigation probability, the TA could ensure the security of MANET routing at a reduced cost. To improve the efficiency, detection probability is correlated with a node's reputation that allows a dynamic detection probability determined by the trust of the users. The extensive analyze is simulated and the results show that the proposed scheme substantiates the effectiveness and efficiency of the system.

Keywords: - Mobile Ad-hoc Networks (MANETs), Probabilistic Misbehavior Detection, Trusted Authority (TA), Inspection Game.

1. INTRODUTION

Mobile ad hoc network (MANET) [1] consists of a set of wireless mobile nodes communicating with each other without any centralized control or fixed network infrastructure. MANETs have been evolving to serve a growing number of applications that rely on multi hop wireless infrastructures that can be deployed quickly. Today, advances in wireless technologies [2], Bluetooth [3], and third-generation cellular have led to a proliferation of mobile ad-hoc. The number of mobile Internet devices is expected to reach a billion in the near future [4] and exceed the number of stationary nodes.

Mobile Ad-Hoc Networks (MANETs) are vulnerable to several types of attacks including passive eavesdrop-ping, jamming, compromising (capturing and reprogramming) of the nodes, and insertion of malicious nodes into the Network. Widespread adoption of ad-hoc networks, particularity for mission critical tasks, hinges to the development of strong protection mechanisms against that attacks. Due to the scarcity of resources, traditional ad-hoc network security solutions are not viable for MANETs. it also increases the connectivity of the networks. which may be important as node mobility increases. Results in [5]–[7] show that when the number of nodes is small.

Moreover, size and cost constraints of the nodes limit their memory size and processing power. Therefore, security solutions which demand successive processing, storage or communication overhead are does not practical's. In particular, their high computational complexity and public key ciphers are not suitable for ad-hoc networks.

Here, we present our adversaries and attack models as well as the network assumptions and the node model.

1.1 Adversaries and Attack Models

The attackers outside the network do not know the secret keys, but those inside the network may know the keys. We classify their attacks according to their behaviors (e.g., active or passive) and locations (e.g., inside or outside the network).

1.2 For Security Primitives

1.2.1 Digital Signature:

We consider the entire network **T** a group and each node has a pair of group public/private keys issued by the group manager. The group public key, which is denoted by GT+, is the same for all the nodes in **T**, whereas the group private key, which is denoted by GA− (for A ∈ **T**), is different for each node. Node A may sign a message with its private key GA−, and this message can be decrypted via the public key GT+ by the other nodes in **T**, which keeps the anonymity of A [14]. We also assume that there exists a dynamic key management scheme working together with the admission control function of the network, which enables the group signature mechanism running properly. Such assumptions are also adopted in the existing work of military ad hoc networks [17].

1.2.2 Comparison between Repudiation And Non-Repudiation:

In Existing System MANETs, a node could misbehave by dropping packets intentionally even when it has the capability to forward the data (e.g., sufficient buffers and meeting opportunities Routing misbehavior can be caused by selfish (or rational) nodes that try to maximize their own benefits by enjoying the services provided by MANET while refusing to forward the node for others or malicious nodes that drop packets or modifying the packets to launch attacks. Then show that routing misbehavior will significantly reduce the packet delivery rate and thus pose a serious threat against the network performance of MANET. Therefore, a misbehavior detection and mitigation protocol is highly desirable to assure the secure MANET routing as well as the establishment of the trust among nodes in MANETs.
The problem in misbehaviors detection in ad-hoc networks is that most of which are based on forwarding history verification, which are terms of transmission overhead and verification cost high. The securities overhead incurred by forwarding history checking is critical for a MANETs since expensive security operations will be translated into more energy contributed. which can be represents a fundamental challenge in resource constrained MANETs.

2. RELATED WORK

Existing routing algorithms for ad-hoc Networks assume that nodes are willing to forward packets for others. In the real world, however, most people are socially selfish; i.e., they are willing to forwarded nodes with which they have social ties but not others, such willingness varies with the strength of the social tie. Following the philosophy of design for user, a Social Selfishness Aware Routing (SSAR) algorithm is proposed to allow user selfishness and provide better routing performance in an efficient way. To select a forwarding node, SSAR considers both users' willingness to forward and their contact opportunity, resulting in a better forwarding strategy than purely contact-based approaches. Moreover, SSAR formulates the data forwarding process as a Multiple Knapsack Problem with Assignment Restrictions (MKPAR) to satisfy user demands for selfishness and performance.

In the first category, the common practice is to secure the popular on-demand routing protocols, such as ad hoc on-demand distance vector routing (AODV) [5], destination sequenced distance vector (DSDV) [6] and [7], by using a security association between the source and destination nodes such as pair wise secret keys and end-to-end authentication [4]. Hence (SEAD) [10], and Authenticated Routing for Ad-hoc Networks (ARAN) [11]. SAODV is a direct extension of AODV that uses a digital signature to sign routing messages and hash chains to secure hop counts [8], which is expensive for MANETs. Some security features to prevent attackers from tampering routing information and some other types of attacks such as DOS [9]. it requires some extent of time synchronization among the nodes in a MANET [15]. SEAD is based on DSDV and uses one-way hash chains to authenticate hop counts and sequence numbers of routing messages [10]. The security mechanism in SEAD can be TESLA or the shared secret keys between each pair of nodes. ARAN uses a digital signature to provide end-to end authentication and provides node authentication, message integrity, and non-repudiation services [11]. During route discovery, each routing message is signed by a source node and then broadcast to others.
Routing protocol, it can work with both AODV and SSAR. In the second category, protecting routing traffic against specific attacks is their major purpose. These include Network layer Protocol with Byzantine Robustness [18] for Byzantine failure and its extension to large data networks using hierarchical routing [19].

Mobile Ad-hoc Networks (MANETs) have been identified as one of the key areas in the field of wireless networks. They are characterized by large end-to-end

communication latency and the lack of end-to-end path from a source to its destination. The main objective of this paper is to develop a robust trust mechanism and an efficient and low cost malicious node detection technique for MANETs. The results indicate that the proposed scheme provides high data availability and packet-delivery ratio with low latency in MANETs under adversary attacks.

3. PROPOSED SYSTEM

The Proposed System consists of the misbehavior detection and incentive scheme as a single framework (i-Believe). The i-Believe scheme is inspired from the Inspection Game theory model in which an inspector verifies if another party are called inspected, ad-hoc to certain legal rules.

In this model, the inspected has a potential interest in violating the rules while the inspector may have to perform the partial verification due to the limited verification resources. Finally, the inspector could take advantage of partial verification and corresponding punishment to discourage the misbehaviors of inspected. Furthermore, the inspector could check the inspected with a higher probability than the Nash Equilibrium points to prevent the offences, as the inspected must choose to completely the rules due to its rationality. Hence, it is crucial to guarantee that the acknowledgment packets are valid and authentic. The benefit of iBelieve is a Probabilistic Misbehavior Detection Scheme to achieve efficient trust establishment in MANETs.

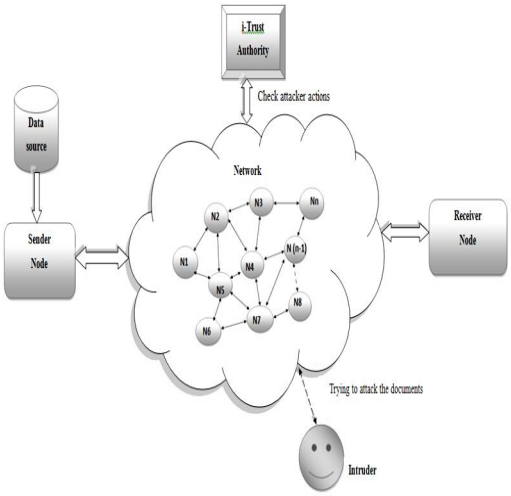

Fig no.1.System Architecture

Firstly, a general misbehavior detection framework is proposed based on a series of newly introduced data forwarding evidences. The evidence framework not only detects various misbehaviors but also be compatible to various routing protocols.

3.1 Probabilistic Misbehavior Detection Algorithm

Step1: Start the task and send the node N1,N2;
Step2: Check any node drop the datas
Step3: If R!=0 than return 1;
Step4: Else if Nk(m)< R and Moduls of Nk(m)<D than return 1;
Step5: End procedure;

Step1: Initialize the number of nodes n;
Step2: For i<- 1to n do
Step3: Generate a random number mi from 9 to 10n-1
Step4: If mi/10n<pb then
Step5: Ask all the nodes 9including node i)to provide evidence about node i
Step6: If basic detection (I,task,)
Step7: Then give a punishment C t node i
Step8: Else pay node I the compension w
Step9: End

3.2 Performance Analysis

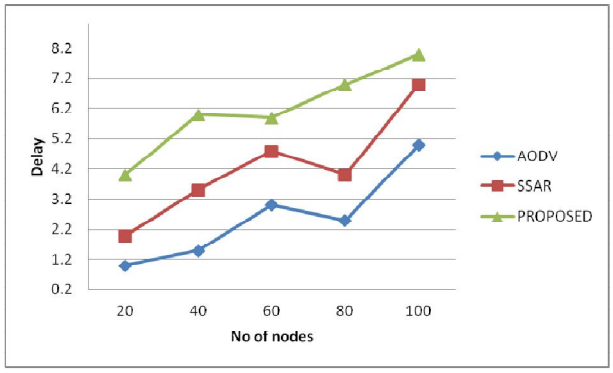

Fig 2. Detected rate delay in multiple nodes

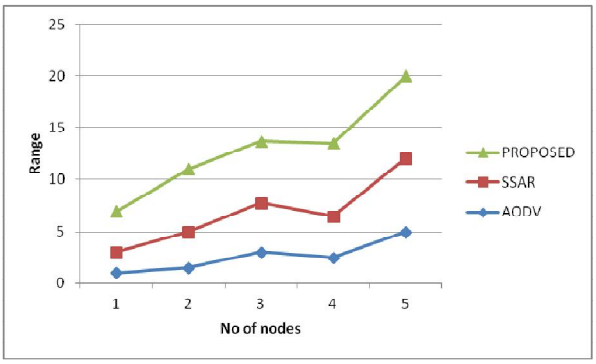

Fig 3. Range between transferred nodes

The result set up the experiment environment with the opportunistic networking environment (The ONE) simulator [20], which is designed for evaluating DTN routing and application protocols. In this paper adopt the First Contact routing protocol, which is a routing mechanism and use our campus map Fig 1.0 as the experiment environment. We set the time interval to be about 3 hours as the default value, and this paper AODV, SSAR nodes on the map, respectively. Finally this each parameter setting an conduct the experiment for 100 nodes.

If a node's PLR is 0, we take it as a normal node. Further, if0< PLR <1, the node could launch a gray hole attack by selectively dropping the packets. In our measured, we use the detected rate of the malicious nodes to measure the effectiveness of iBelieve Fig 2.0 take all the nodes whose PLR larger than 0 as the malicious ones. On the another side, since a normal node may also be identified as the malicious one due to the depletion of its buffer, we need to measure the false alert of iBelieve and show that iBelieve has little impact on the normal users who adhere to the security nodes. Thus, we use the misidentified rate to measure the false negative rate. Moreover, we evaluate the transmission over head Cost transmission and verification overhead Cost verification in terms of the number of evidence transmission and verification for misbehavior detection. In thus, we will evaluate the effectiveness of iBelieve under different parameter settings.

4. CONCLUSION

This propose probabilistic misbehavior detection scheme (I Believe), which could reduce the detection overhead effectively. This paper model it as the inspection game and show that an appropriate probability setting could assure the security of the Ad-hoc networks at a reduced detection overhead. Our simulation results confirm that I Believe will reduce transmission overhead and range incurred by misbehavior detection and detect the malicious nodes effectively performed. Our future work will focus on the extension of I Believe to other kind of networks The trust management mechanism enables each network node to determine the trustworthiness of the nodes that it had a direct transaction . On the other hand, ITRM takes advantage of an iterative mechanism to detects and isolate the malicious nodes from the network in a short time. The proposed scheme and showed that it effectively detects the malicious nodes even in the presence of the attacks on the trust and detection mechanisms. Moreover, using computer simulations showed that the proposed mechanism provides high data availability with low latency.

REFERENCES

[1]. *S. Corson and J. Macker," Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations ,IETF RFC 2501, Jan. 1999.*

[2]. *Wireless LAN medium access control (MAC) and physical layer (PHY) specifications , ISO/IEC 8802-11; ANSI/IEEE Standard 802.11, Aug. 1999.*

[3]. *Bluetooth Core Specification, v1.2, Nov. 2003.*

[4]. *C. E. Perkins, J. T. Malinen, R. Wakikawa, A. Nilsson, and A. J. Tuominen," Internet connectivity for mobile ad hoc networks," J. Wireless Commun. Mobile Comput., vol. 2, no. 5, pp. 465–482, Aug.2002.*

[5]. *E. M. Royer, P. M. Melliar-Smith, and L. E. Moser,"An analysis of the optimum node density for ad hoc mobile networks,"inProc. IEEE ICC,Helsinki, Finland, June 2001, pp. 857–861.*

[6]. *M. Sanchez, P. Manzoni, and Z. J. Haas,"Determination of critical trans-mission range in ad-hoc networks,"inProc. Multiaccess Mobility and Teletraffic Wireless Communications 1999 Workshop (MMT), Venice,Italy, Oct. 1999, pp. 293–304.*

[7]. *L. Kleinrock and J. Silvester,"Optimum transmission radii for packet radio networks or why six is a magic number," in Proc. IEEE Nat. Telecommunications Conf., 1978, pp. 431–435.*

[8]. *S. T. Sheu and J. Chen, "A novel delay-oriented shortest path routingprotocol or mobile ad-hoc networks," in Proc. IEEE ICC, Helsinki, Fin-land, June 2001, pp. 1930–1934.*

[9]. *C. E. Perkins, E. Belding-Royer, and S. R. Das, "Ad-hoc on-demand distance vector (AODV) routing," IETF RFC 3561, July 2003.*

[10]. *D. B. Johnson, D. A. Maltz, and Y. C. Hu, "The dynamic source routing protocol for mobile ad hoc networks (DSR).*

[11]. *R. Lu, X. Lin, H. Zhu, and X. Shen, "SPARK: A New VANET-based Smart Parking Scheme for Large*

Parking Lots", in Proc. of IEEE INFOCOM'09, Rio de Janeiro, Brazil, April 19-25, 2009.

[12]. T. Hossmann, T. Spyropoulos, and F. Legendre, "Know The Neighbor: Towards Optimal Mapping of Contacts to Social Graphs for MANET Routing", in Proc. of IEEE INFOCOM'10, 2010.

[13]. Q. Li, S. Zhu, G. Cao, "Routing in Socially Selfish Delay Tolerant Networks" in Proc. of IEEE Infocom'10, 2010.

[14]. H. Zhu, X. Lin, R. Lu, Y. Fan and X. Shen,"SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks," in IEEE Transactions on Vehicular Technology,vol.58,no.8,pp.828-836,2009.

[15]. E. Ayday, H. Lee and F. Fekri,"Trust Management and Adversary Detection for Delay Tolerant Networks," in Milcom'10, 2010.

[16]. R. Lu, X. Lin, H. Zhu and X. Shen,"Pi: a practical incentive protocol for delay tolerant networks," in IEEE Transactions onWirelessCommunications,vol.9,no.4,pp.1483-1493,2010.[7]F.Li, A. Srinivasan and J. Wu, "Thwarting Blackhole Attacks in Disruption-Tolerant Networks using Encounter Tickets," in Proc. of IEEE INFOCOM'09, 2009.

[17]. Fudenburg,"Game Theory",p17-18,example1.7:inspection game.

[18]. M. Rayay, M. H. Manshaeiy, M. Flegyhziz, J. Hubauxy"Revocation Games in Ephemeral Networks" in CCS'08,2008.

[19]. S. Reidt, M. Srivatsa, S. Balfe,"The Fable of the Bees:Incentivizing Robust Revocation Decision Making in Ad Hoc Networks" in CCS'09, 2009.

[20].