Efficient Content Authentication in Ad-Hoc Networks- Mitigating DDoS Attacks

Anuj Joshi Krishna Kant Agrawal Dr. Deepak Arora Shashwat Shukla

Department of Computer Science & Engineering, Amity University
Uttar Pradesh, Lucknow , India

ABSTRACT
With the emergence of mobile ad hoc networks it is now possible to access network accessing and communicate data in an area where no fixed infrastructure exists or existing infrastructure is not available. Since in ad hoc networks, the exact copies of the same content are stored at various locations. Therefore in order to prevent from various attacks based on the content; it becomes important to have some security solutions. In this paper, we propose an efficient content authentication method in ad hoc network. Foremost, the challenges in ad hoc networks have been mentioned in this paper. This paper focuses on secure packet forwarding in ad hoc networks and proposes a new solution based on observation by all the neighboring nodes to mitigate the effects of adverse situations caused by malicious nodes. This prevention mechanism exploits all well-behaving nodes' local knowledge to bypass misbehaving nodes, evaluate path quality and choose the most reliable path for data forwarding. In this paper, a new solution for mobile ad hoc networks based on observation by all the neighboring nodes is presented.

General Terms
Content Authentication, MANETs

Keywords
Ad hoc Networks, DDoS, Misbehaving Nodes, Optimal Route

1. INTRODUCTION
In ad hoc network environment peers are connecting or disconnecting to the environment, which means this environment is dynamic. Therefore, the security issues become very important in this scenario. Authentication is the process of verifying the identity of an entity. Similarly in a peer-to-peer system a verification that the node some peer is communicating with really is who it claims to be [5].

1.1 Challenges in ad hoc networks
To distribute content to users, a peer-to-peer network must be able to locate content, scale to a useful size, and provide reliable operation.

1.1.1. Locating Content
A problem that arises in ad hoc networks during file sharing is to locate content that matches user requests. To distribute content to users, a mobile ad hoc network must be able to locate content, scale to a useful size, and provide reliable operation [8].

1.1.2. Content integrity
It is the primary trust issue in a content delivery network. If the original content is tampered with or altered during storage, transport, or delivery, the requester is misled and the reputation of the author is unfairly and unknowingly tarnished. It is important for both the author and the requester to ensure that the content the requester receives is an exact copy of the content the author originally created [8].

2. CONTENT AUTHENTICATION IN AD HOC NETWORKS

An attractive distinctive feature in ad hoc file sharing scenarios is the possibility of replicating the same content among different nodes, and download a specific content at any moment, Once a user gets the file, it is usual that a local copy will remain in the node, in such a way that future queries will identify the node as one of the various locations from which the content can be obtained. This fact presents some interesting properties. For the same content resides at different locations, an application can grant priority to that which offers a less expensive path (e.g. in terms of bandwidth and/or number of network hops.). If some parts of the network are temporarily disconnected then to some extent, fault tolerance may also be guaranteed through this replication. In a collaborative working environment, the previous features are highly desirable [1]. However, it is unrealistic to assume that every joining node will exhibit a honest behavior, even if they have always behaved correctly in the past. Once that a content is replicated through different locations, the originator loses control over it. A malicious party can modify the replica according to several purposes:

1. To claim ownership over the content.
2. To insert malicious software into a highly demanded content.
3. To boycott the system by offering fake contents.

Eventually, this can generate distrust and bad reputation in the community [9]. Therefore, secure content distribution protocols are highly desired for such environments. Briefly, the main objective of content authentication protocol is to maintain content integrity, ensuring its authenticity and avoiding non-authorized content alterations.

3. A GROWING NETWORK THREAT--DDOS

Distributed Denial of Services (DDoS) attacks target web sites, hosted applications or network infrastructures by absorbing all available bandwidth and disrupting access for legitimate customers and partners [6]. DDoS attacks can bring mission critical systems and business operations to a halt, resulting in lost revenue opportunities, decreased productivity or damage to your reputation. It becomes important to study and analyze security in ad hoc networks for emphasizing on the lack of practical security mechanisms in fully decentralized and highly dynamic networks. The major problems range from the absence of content authentication mechanisms, which address and assure the authenticity and integrity of the resources shared by networking nodes, to access control proposals, which provide authorization services. In particular, the combination of both, authentication and access control, within well-known file sharing systems may involve several advances in the content replication and distribution processes [7]. The DDoS attackers hijack secondary victim systems using them to wage a coordinated large-scale attack against primary victim systems. As new countermeasures are developed to prevent or mitigate DDoS attacks, attackers are constantly developing new methods to circumvent these new countermeasures. DDoS attacks are relatively new and not well understood.

4. SECURE ROUTING

The basic requirement in ad hoc networks is to organize and adapt the self organized behavior of the participating nodes and the maintenance of an infrastructure less network .The basic principles to provide self-organization are to dynamically discover potential communication nodes and available services (generally starting from a few basic mechanisms such as broadcasting), and efficiently navigate with independence of the physical network [2].There are various questions pertaining to the assumptions on the network con-figuration that would limit its self-organizing nature and therefore its degree of adaptively and robustness. There is no pre-deployed infrastructure is available for routing packets. In ad hoc wireless network, instead routing relies on intermediary nodes completely agreed to route messages for each other. Therefore all networking functions are performed by the nodes themselves in a self-organizing way. This operating principle involves cooperation among nodes as an essential requirement [3].

4.1 Misbehaving Nodes

There are two kinds of misbehaving nodes [12]:

Malicious nodes

For malicious nodes, they behave cooperatively during the route discovery phase, and then they are included in some discovered routes. But they drop data packets in the data delivery phase if these packets are not intended for themselves. As a consequence, data packets delivered over routes containing these malicious nodes will be lost. In most simulations, malicious nodes drop all data packets passing through them. But in order to deal with potential misbehaving nodes that are difficult to detect, the situations in which those nodes drop data packets at a certain probabilities are also considered.

Selfish nodes

For selfish nodes, they drop all packets during a simulation. Because route request packets are also dropped by these nodes, they will not be included in any discovered routes. Therefore, no data packets will pass through them.

4.2Misbehaving Node Detection

Misbehaving node detection includes neighbor sensing, packet forwarding monitoring [11].

4.2.1. Neighbor Sensing

Neighbor sensing is used to detect immediate neighbors of a node, and is the precondition of neighbor behavior monitoring and calculation based on the observation of traffic and content by all the neighboring nodes. There are several reasons for neighbor sensing.

1. Due to lack of a central management agent, only fully distributed monitoring and management techniques can be employed in mobile ad hoc networks. Therefore each node should be responsible for monitoring its neighboring nodes in order to detect any abnormal behaviors. To perform this kind of operations, a node must know exactly which nodes are its immediate neighbors to be able to monitor their behaviors.

2. In order to prevent selfish nodes keeping silent (dropping all packets) to save energy, a node only provides packet forwarding service to its current neighbors that claim their existences. It means that if a node wants its neighbors to forward its own packets, it has to first claim its existence to its neighbors. As a consequence, each node in the network can be detected and monitored by other nodes.

4.2.2. Packet Forwarding Monitoring

Each node independently performs the monitoring operation within its radio transmission range. Theoretically, a variety of neighbors' behaviors can be monitored and corresponding detected data can be maintained and processed to discover misbehaving nodes. However, to make the neighbor monitoring mechanism effective and suitable for mobile ad hoc networks, the monitoring mechanism should be based on the frequent and

primary behaviors of mobile nodes. For mobile ad hoc networks, its unique characteristic is that each node is responsible for forwarding packets for other nodes. And for secure data forwarding in mobile ad hoc networks, the most important requirement is to ensure that every data packet can reach its destination, which means that each intermediate node must behave cooperatively to forward packets to the next correct node. Only when the requirement that packets can reach destinations is realized, other secure requirements such as data integrity and confidentiality will be useful and make sense. Therefore, the packet forwarding behavior is the most important behavior in mobile ad hoc network, and should be monitored primarily. And it is also the only thing that can be used to detect selfish nodes in mobile ad hoc networks. And also due to limited available resources of each mobile device, such as memory, energy, in order to decrease the corresponding computation and transmission overhead caused by monitoring operation, other behaviors are not considered in this solution currently.

4.2.3. Evaluation Criteria for Well-behaving Nodes

Observations by the neighboring nodes are calculated based on a node's packet forwarding ratio, which means if node A sends a packet to node B (B is an intermediate neighbor of A), what is the probability that the packet will be forwarded cooperatively by B and reach the next node. Packet forwarding ratio (PFR) is the criterion in this solution to evaluate a node's local reputation and is quite suitable for secure data forwarding evaluation. Because the most important requirement of secure data forwarding is to make sure that each intermediate node behaves cooperatively to forward the packet and then the packet can reach the destination along the correct route [4].

4.2.4. Monitoring Implementation

The promiscuous mode [14] enables each node to monitor its neighbors' behaviors by overhearing their transmissions. Promiscuous mode means if node A is in the transmit coverage of node B; A can overhear packets from B even if those packets are not directly related to A. So a node can listen to every packet sent by its neighboring nodes, and through which its neighbors' behaviors can be monitored. Each node in the network has a neighbor table which contains relevant information about its entire neighbors. And each node calculates its neighbors' local reputations according to its own observation. In order to keep track of the data packet forwarding behaviors of its neighboring nodes, two basic numbers are maintained and updated for each neighbor.

1. RtF (request to forward) :The number of packets this node has sent to a neighbor (node N) for forwarding in a period of time.
2. RbN (relayed by neighbor) This number is used to show how many packets have relayed cooperatively by Node N in a period of time.

The packet forwarding ratio (PFR) can be expressed based on these two numbers. The packet forwarding ratio is calculated and updated in the following way. In a new period of time, the two numbers are initialized to 0. And when node A sends a packet to node B and requires B to forward this packet, it increases the value of RtFA(B) by one. And A keeps this packet in its cache, and starts to listen to the wireless channel and check whether node B forwards the packet as expected.

After A detects that B relays this packet cooperatively, it increases RbNA(B) by one. Given these two numbers, node A can create a packet forwarding ratio for its neighbor B in this period of time.

$$PFR_A(B) = RbN_A(B) / RtF_A(B)$$

4.2.5 Optimal Route Discovery

Observations of the nodes and their neighbors are used to evaluate the quality of each discovered path at the route evaluation stage. There are some reasons for optimal route discovery. Above all, it is impossible to detect all misbehaving nodes in the network. For example, a selfish node may drop packets at a certain probability which is a litter higher than the predefined threshold, so it will be very difficult to detect such selfish node. If we increase the threshold, some well-behaving nodes may be regarded as misbehaving node due to some other reasons such as collision. Furthermore, data loss may happen because of other reasons. For example, if a rapidly moving node is included as an intermediate node, the packets delivered on this route are more likely to be lost because this node frequently moves outside of its neighbor's radio transmission range. On the contrary, a fixed or rarely moving node is much more reliable for data forwarding. And if a node becomes a bottleneck, the packets passing through this node are more likely to be dropped due to buffer overflow. Additionally, mobile devices with more resources including CPU capability, battery power and memory are more suitable for data forwarding. Therefore, even without regarding misbehaving nodes, different routes could have various performances. How to measure the quality of a discovered path is a big challenge in ad hoc networks.

5. PERFORMANCE EVALUATION

In this section, the simulation results are presented and analyzed. From the results, we could find that misbehaving nodes do degrade the network performance. And the simulation result also supports our belief and display the improvement of network performance when the prevention technique is employed in the route discovery phase. Network simulation is a basic method to perform network technology research. During the research, it may be very difficult or even impossible to implement a network system in a real environment due to various reasons, such as high cost or difficulty of creating the expected environment [15]. Therefore, network simulation becomes a suitable, rapid and cost-effective method to execute performance evaluation. And it

enables researchers to take advantage of other existing solutions and technologies conveniently, and to focus more on their own research topics without paying unnecessary attentions to other parts of the system. NS [10] is open source and free, so it is always growing to include new protocols. NS-2 could be used to evaluate the performance of a variety of network protocols and architectures designed for both wired and wireless networks, and it is suitable to run large scale experiments which are difficult to realize in real environments.

5.1 Simulation Configuration

All simulations take place in a flat square with 1000 meters on each side, and there are 50 mobile nodes in the network. The Distributed Coordination Function (DCF) of IEEE 802.11 is used as the medium access control layer protocol, and the TwoRayGround model is chosen as the radio propagation model. The values of relevant parameters are set to their default values. The radio transmission range of each node is 250 meters and the transmission data rate is set to 2 Mbits/s. DSR is employed as the routing protocol, and CMUPriQueue is used as the interface queue in which at most 50 packets could exist. Due to different concerns in different simulations, some simulation parameters are modified in each simulation. The simulations are performed to evaluate the impact of dynamic network topology. Packet delivery ratio is used to evaluate the network performance. It is the ratio of the number of data packets successfully delivered to all destinations and the number of packets generated by all senders.

5.2 Experimental Output

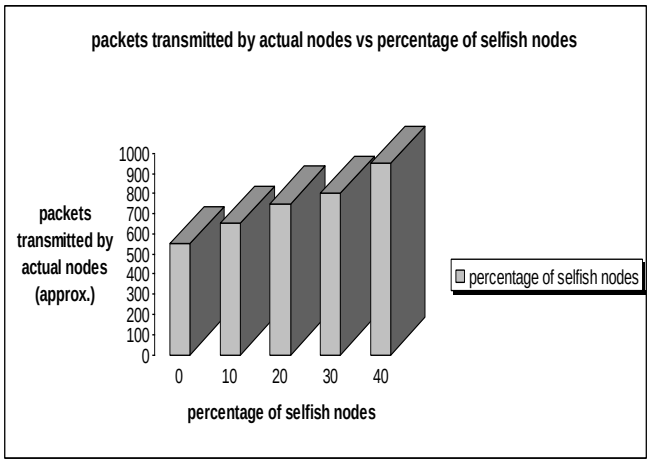

Fig 1. Packets transmitted by actual nodes vs. percentage of selfish nodes

In fig 1., the simulation results show that if there is no selfish node in the network, each well-behaving node relays on an average 550 packets as intermediate node in a simulation. With the increase of selfish nodes, each well-behaving needs to relay more packets (total traffic in the network does not change). Due to all selfish nodes refuse to forward packets, well-behaving nodes need to forward those data packets which should be forwarded by those selfish nodes originally. We can see when 40% nodes in a network are selfish nodes, a well-behaving node needs to forward about 950 packets. Therefore, a well-behaving node's transmission burden will significantly increase if there are a large number of selfish nodes in the network.

5.3 Optimal Route Discovery

The optimal route discovery technique could be used to provide better performance if there are some potential misbehaving nodes in the network that can not be detected or packets are lost due to collision or congestion [13]. It chooses routes according to hop count as well as path quality. In all simulations, constant bit rate is used as the traffic overload. Therefore, no retransmission happen if packet is lost on the way. In order to reduce the impact of other things that cause packet loss, the maximum speed of each node in the simulation is set to 2 m/s, because in such scenario, the packet delivery ratio is about 99.6%. The malicious nodes forward data packets at the probability of 70%. The packet delivery ratio is evaluated in the following situations in which 10%, 20%, 30% and 40% of nodes are malicious nodes respectively. If we suppose that 70% packet forwarding ratio is acceptable, these misbehaving nodes will not be detected. As a consequence, they will be included in some discovered routes. However, a sender node can take advantage of the optimal route discovery technique to find the most reliable route to another node.

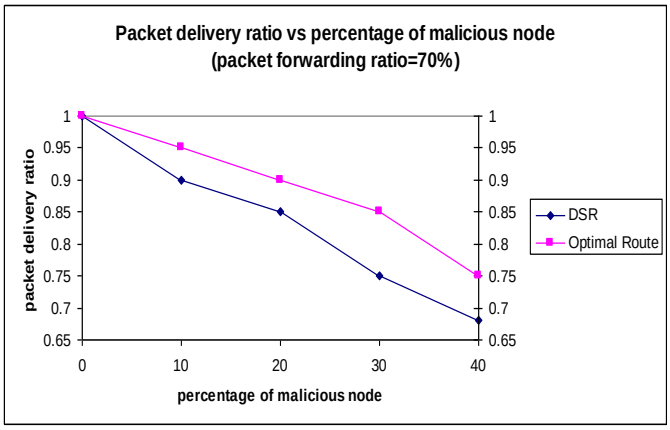

Fig 2. Packet delivery ratio vs. percentage of malicious nodes Packet forwarding ratio: 70%

In fig 2, we can see that the observation mechanism could improve the packet delivery ratio. But compare with the prevention mechanism (bypassing detected misbehaving nodes), the improvement is not so significant, because in these scenarios, the potential malicious nodes do not drop all packets, but drop packets at some probabilities. Therefore, even without this mechanism, the packet delivery ratio is still on an acceptable level. For example, when 40% such malicious nodes exist in the network, the packet delivery ratio is still above 70%.

6. CONCLUSION

Ad hoc Networks are an increasingly promising area of research with practical network technologies and architectures. But due to their specific characteristics such as multi-hop and infrastructure-independent, they are more vulnerable than traditional networks. Various attacks especially those related to routing and forwarding are much easy to be launched by misbehaving nodes in ad hoc networks. By performing neighbor monitoring and information exchange misbehaving nodes could be effectively detected. The simulation shows that malicious nodes degrade the network performance considerably and selfish nodes increase other nodes' burdens. Thus we can say that when the malicious nodes have been detected these will not be in the optimal path and hence various attacks such as DDoS can be prevented. Once we have an optimal route from the source to the destination (no misbehaving nodes) the content can not be tampered and its integrity can be maintained, hence authentication is efficient and correct. We have explored the based on the observations of the network traffic and data packets routing by all the neighboring nodes we evaluate the nature of misbehaving nodes.

7. FUTURE DIRECTION

Ad hoc systems are rapidly maturing from being arrowly associated with copyright violations, to a technology that offers tremendous potential to deploy new services over the Internet. Other possible monitoring and calculation based on the observation methods should be investigated, such as end-to-end performance evaluation technique. However, it results in a large quantity of computation and transmission overheads currently. Therefore, it needs to be optimized to reduce its overhead. Furthermore, some potential security problems exist in this scheme, for example a misbehaving node could first behave cooperatively to get high monitoring and then begins to broadcast false monitoring information to disrupt the network. Something must be done to address these security problems. Distributed Denial of Service (DDoS) attacks have become a large problem for users of computer systems connected to the Internet. As new countermeasures are developed to prevent or mitigate DDoS attacks, attackers are constantly developing new methods to circumvent these new countermeasures.

8. ACKNOWLEDGEMENT

First and foremost, I would like to express my heartiest gratitude to our honorable faculty members for their suggestions, guidance, constant encouragement and enduring patience throughout the progress of the research paper. I would also like to express my sincere thanks for their advices and all-out cooperation.

9. REFERENCE

[1] X. Zhang, S. Chen, and R. Sandhu. Enhancing data authenticity and integrity in ad hoc systems. *IEEE Internet Computing*, pages 42–49, November–December 2005.

[2] F. Zambonelli, M. Gleizesb, M. Mameia, and R. Tolksdorf. Spray computers: Explorations in self-organization. *Pervasive and Mobile Computing*, 1:1–20, March 2005.

[3] V. Srinivasan, P. Nuggehalli, C. Chiasserini, and R. Rao. Cooperation in wireless ad hoc networks. In *Proceedings of IEEE Infocom*, 2003.

[4] L. Buttyán and J.-P. Hubaux. Stimulating cooperation in self-organizing mobile ad hoc networks. *Mobile Networks and Applications*, 8:579–592, 2003.

[5] J. Lopez, R. Oppliger, and G. Pernul. Authentication and authorization infrastructures (aais): A comparative survey. *Computer Communications*, 27(16):1608–1616, October 2004.

[6] V. Paxson. An analysis of using reflectors for distributed denial-of-service attacks. Computer Communication Review 31(3), July 2001.

[7] E. Palomar, J.M. Estevez-Tapiador, J.C. Hernandez-Castro, and A. Ribagorda. Secure content access and replication in pure ad hoc networks *Computer Communications*, 31(2):266–279, February 2008.

[8] B. Zhu, S. Jajodia, and M.S. Kankanhalli. Building trust in peer-topeer systems: a review. *International Journal of Security and Networks*, 1(1/2):103–112, 2006.

[9] H. Luo and S. Lu. Ubiquitous and robust authentication services for ad hoc wireless networks. Technical report, 2000.

[10] The Network Simulator - ns-2. http://www.isi.edu/nsnam/ns/index.html.

[11] Panagiotis Papadimitratos and Zygmunt J. Haas, "Secure routing for mobile ad hoc networks", In Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 27-31, 2002

[12] Lidong Zhou and Zygmunt J. Haas, "Securing ad hoc networks", IEEE network, special issue on network security, November/December, 1999.

[13] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," Proceeding of MOBICOM, Aug 2000.

[14] P. Papadimitrators, Z. J. Haas, "Secure message transmission in mobile ad hoc networks", Ad Hoc Networks (2003) 193-209.

[15] P. Michiardi, R. Molva, "Simulation-based analysis of security exposures in mobile ad hoc networks", European Wireless Conference, 2002.