ISSN:2348-2079

Volume-6 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

A Hierarchical OLSR Social Norm Incentives for Network Coding In MANETS

[1]Nancy P, [2]Abirami D, [3]Kiruthika N, [4]C. Dharanya

Department of Computer Science and Engineering,Velalar College of Engineering and Technology
[1] Assistant Professor, [2-3]UG Students

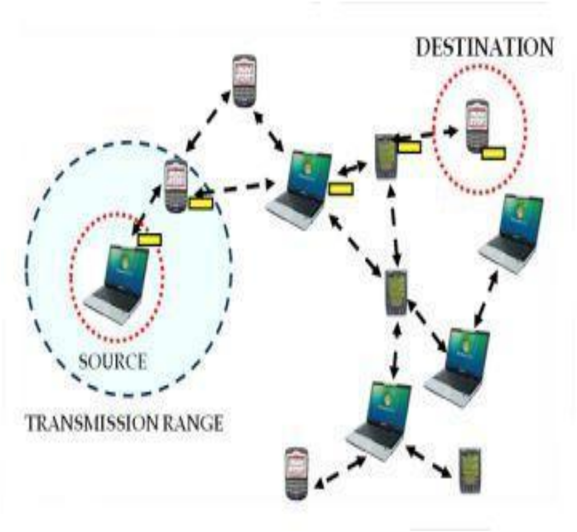
E-mail id : [1] nancipeter@gmail.com , [2] abi241997@gmail.com , [3] kiruthikamahe@gmail.com

Abstract--The performance of mobile ad hoc network transmissions subject to disruption, interference, and jamming can be improved by using the concept of network coding.By focusing on the Optimized Link State Routing (OLSR) protocol, an IDS mechanism to accurately detect and isolate misbehavior node(s) in OLSR protocol based on End-to-End (E2E) communication between the source and the destination is proposed. The collaboration of group of neighbor nodes is used to make accurate decisions. Creating and broadcasting attackers list to neighbor nodes enables other node to isolate misbehavior nodes. Eliminating misbehavior nodes allow the source to select another path to its destination. The simulation results show that the proposed mechanism is able to detect any number of attackers while keeping low overhead in terms of network traffic. The conditions for the sustainability (or compliance) of the social norm are identified, and a sustainable social norm that maximizes the social utility is designed via selecting the optimal design parameters, including the social strategy, reputation threshold, reputation update frequency, and the generation size of network coding. Finally, practical issues, including distributed reputation dissemination and the existence of altruistic and malicious users, are discussed.

Index terms-- Misbehavior nodes, Network coding,Reputation, Social norm

I. INTRODUCTION

A computer network is a telecommunication community which permits computer systems to trade facts. In computer networks, computing devices exchange information with each other the usage of a data hyperlink. The connection between nodes is set up using either cable media or wireless media. A Mobile Adhoc Networks is a spontaneous web that can be instituted with no constant infrastructure. All its nodes behave as routers in this way and seize component in its invention and renovation of paths to supplementary nodes inside the net Security in Mobile ad-hoc networks is tough to accomplish due to vibrantly changing and absolutely decentralized topology as well as the vulnerabilities and boundaries of wireless data transmissions. A MANETs (Mobile Adhoc Networks) consists of a large range of sensors, each of that is physically small devices, and are ready with the functionality of sensing the physical environment, records processing, and speaking wirelessly with different sensors. Commonly, we expect that every sensor in a MANETs has positive constraints with respect to its power supply, energy, memory, and computational competencies. One of the distinct characteristics of MANETs is that everygiving nodes need to be encompassed in the routing manner.



II. PROBLEM DEFINITION

Every time the network imparting load is greater than the community capacity causes the reputation on the deadlock scenario. At some stage in transmission, too many packets are misplaced.It is to find out the supply of nodes to transmit the packet to the nodes.When too many packets are transmitted via the network, reputation happens at very excessive traffic.Reputation manage is to keep away from the reputation collapse inside the network and to modify the float of the packets with the constant variable length to keep away from the hassle that takes place whilst transmitting the packets to the node.As deployment sizes and facts charges grow, reputation arises as a major problem in these networks. This reputation results in indiscriminate dropping of facts, i.e. facts of high significance is probably dropped at the same time as others of much less importance are added.Network reputation results in packet loss, throughput impairment, extra network lifetime, much less packet delivery ratio and energy waste.

III. LITERATURE REVIEW

1. Social Norm Incentives for Secure Network Coding in MANETs

In this paper work [1] Chuchu Wu, has proposed the throughput of mobile ad hoc networks subject to disruption, loss and interference can be significantly improved with the use of network coding. However, network coding implies extra work for forwarders. Selfish forwarders may prefer to simply forward packets without coding them because of the processing overhead introduced by network coding. This is especially true in secure network coding where the coded packets are protected from pollution attacks by processor intense homomorphic signatures. To drive selfish nodes to cooperate and encode the packets, this paper introduces social norm based incentives. The social norm consists of a social strategy and a reputation system with reward and punishment connected with node behavior. Packet coding and forwarding is modeled as a repeated alternate gift-giving game. The interaction between nodes in the repeated game is formalized, the conditions for social strategy sustainability (or compliance) are identified, and a sustainable game that optimizes the social welfare is designed. For this game, the impact of packet loss rate, reputation thresholds andreputation update frequency on performance is evaluated. Mobile devices like smart phones are becoming increasingly powerful and capable to function not only as clients, but also as peers in a fully fledged ad hoc network. For instance a mobile may propagate to neighbors in ad hoc mode a stream that it is downloading from the Internet via WiFi or 3G. The mobile devices, however, have energy constraints. Since forwarding other devices' packets provides no benefit to a mobile that is not an intended destination, rather, it consumes battery resources; a self-interested relay node chooses not to forward the packets. If every relay node drops others' packets, the video never gets delivered to friends several hops away. This selfish behavior, however, can backfire — when the selfish node transmits its own video file, it will be treated the same way, i.e. its file will be dropped. This behavior is known as"tit for tat" in cooperative P2P distribution protocols (e.g. bit torrent) and can be corrected with incentives.

2. Practical Defenses against Pollution Attacks in Wireless Network Coding

In this paper work [2] Jing Dong, has proposed recent studies have shown that network coding can provide significant benefits to network protocols, such as increased throughput, reduced network reputation, higher reliability, and lower power consumption. The core principle of network coding is that intermediate nodes actively mix input packets to produce output packets. This mixing subjects network coding systems to a severe security threat, known as a pollution attack, where attacker nodes inject corrupted packets into the network. Corrupted packets propagate in an epidemic manner, depleting network resources and significantly decreasing throughput. Pollution attacks are particularly dangerous in wireless networks, where attackers can easily inject packets or compromise devices due to the increased network vulnerability.

In this article, we address pollution attacks against network coding systems in wireless mesh networks. We demonstrate that previous solutions are impractical in wireless networks, incurring an unacceptable high degradation of throughput. We propose a lightweight scheme, DART that uses time-based authentication in combination with random linear transformations to defend against pollution attacks. We further improve system performance and propose EDART, which enhances DART with an optimistic forwarding scheme. We also propose efficient attacker identification schemes for both DART and EDART that enable quick attacker isolation and the selection of attacker-free paths, achieving additional performance improvement. A detailed security analysis shows that the probability of a polluted packet passing our verification procedure is very low (less than 0.002% in typical settings). Performance results using the well-known MORE protocol and realistic link quality measurements from the Roofnet experimental testbed show that our schemes improve system performance over 20 times compared with previous solutions.

3. FITS: A Finite-Time Reputation System for Cooperation in Wireless Ad-Hoc Networks

In this paper work [3]Tingting Chen, has proposed A wireless ad hoc network does not have an infrastructure and thus needs the cooperation of nodes in forwarding other nodes' packets. Reputation system is an effective approach to give nodes incentives to cooperate in packet forwarding. However, existing reputation systems either lack rigorous analysis, or have analysis in unrealistic models. In this paper, we propose FITS, the first reputation system that has rigorous analysis and guaranteed incentive compatibility in a practical model. FITS has two schemes: the first scheme is very simple, but needs a Perceived Probability Assumption (PPA) ; the second scheme uses more sophisticated techniques to remove the need for PPA. We show that both of these two FITS schemes have a subgame perfect Nash equilibrium in which the packet forwarding probability of every node. Experimental results verify that FITS provides strong incentives for nodes to cooperate.

A wireless ad hoc network does not have an infrastructure. In such a network, the cooperation of nodes is needed for forwarding other nodes' packets. If nodes do not forward each other's packets, the entire wireless ad hoc network cannot function properly. Nevertheless, in civilian ad hoc networks, nodes belong to different users and thus have their own interests. Consequently, we need to give nodes incentives to make them cooperative. There are mainly two approaches to give nodes incentives: reputation-based systems and credit-based systems (see Section 7 for examples of these two types of systems). In this paper, we focus on the reputation-based approach, which is highly efficient and has been effectively applied to wireless ad hoc networks.

The existing works on reputation systems suffer from one of two problems. First, most of them do not have rigorous analysis of incentive-compatibility. Hence, it is not clear what guarantee for cooperation these reputationssystems can provide. Second, although some other reputation systems do have rigorous analysis, their analyses are in unrealistic models. Therefore, in practice, their work cannot guarantee cooperation as well.

IV. SYSTEM ANALYSIS

EXISTING SYSTEM:

In existing system social norm based incentives to encourage nodes in the network to cooperate, aiming at maximizing the transmission performance (packet delivery rate) of the network.Taking the costs (the power consumptions) into account, we use social utility as a metric of the system. Social utility is defined to be the total utility of all nodes in the network after one time period.

Another important metric for an incentive scheme is the obedience of the nodes, i.e., sustainability of the social norm. A social norm will be sustained, i.e., can persist for everleading to a stable solution, when selfish nodes choose to comply with the social strategy σ instead of deviating from it. In our case sustainability is guaranteed when the proper punishment is enforced, namely when an intermediate node will have a long-term utility decrease if it does not perform coding and/or forwarding when it is prescribed to do so. Sustainability reflects the probability that a selfish node will choose to cooperate and help others. The more intermediatenodes perform coding, the higher delivery rate the network will achieve; so the sustainability of the incentive scheme also affects the transmission performance.The reputation update in our scheme lowers the relay node's reputation only when misbehavior (i.e. performing a worse action than the prescribed action) is detected, whereas performing F/NCF when the prescribed action is "drop" does not count for such misbehavior. So prescribing "drop" when the relay node's reputation is low simply allows low reputation nodes to automatically recover their reputation without extra efforts. This strategy is only one among many valid strategies; however, various strategies result in different performancesunder different network conditions.

DRAWBACKS:

- ✓ Network coding is adopted by selfish nodes because of reputation.
- ✓ But network coding is suspectible to pollution attacks.
- ✓ Poor safety.
- ✓ Pollution avoidance schemes are so costly which again makes the node to be selfish.

PROPOSED SYSTEM:

The IDS we propose belongs to specification-based detection with distributed cooperative nodes that are suitable for MANETs. The misbehavior node detection process that we propose validates the communication path then detects and isolates misbehavior nodes in the invalid paths. The proposed IDS uses the collaboration of a group of nodes to make accurate decisions. The successfully detected misbehavior node is added to a black-list which is broadcast to all 1-Neighbors and so on to all network nodes.

Then all neighbor nodes receive this list and it makes another confirmation by sending a

PVM message to the attacker to be certain this node is actually an attacker. After confirmation it resends the black-list to its neighbors with a higher rating. When the neighbor receives this black-list it excludes the attacker from the routing table to ignore attacking attempts. OLSR security vulnerabilities can be summarizedwith watch dog OLSR.

In this project, we are focusing only on traffic relay/generation refusal where the malicious node acts as a black-hole and drops packets. We introduced two types of attackers. The type-1 attacker drops all the received packets. The type-2 attacker is smarter and drops only data packets and exchanges control packets normally. We extended the security of OLSR in two parts. The first part validates the communication path by sending periodic messages. The second part is concerned with finding malicious nodes in the invalid path.

ADVANTAGES:

- ✓ MANETs keep up advert hoc networking and incorporate the capability of self-forming, self-restoration, and self-corporation.

- ✓ Better performance in adaptive congestion avoidance with quality routing while the use of clustering techniques to reduce electricity consumption

- ✓ Progressed dependable routing which affords better protection

- ✓ Low energy needed to deliver the data by using congestion route avoidance enabled.

HARDWARE REQUIREMENTS:

- System : Pentium Core 2 Duo
- Hard Disk : 80 GB
- RAM : 1GB DDR 2
- Keyboard : LG 104 Key keyboard
- Mouse : Logitech Optical mouse
- Monitor : 15 inch TFT Monitor

SOFTWARE REQUIREMENTS:

- Operating System : Windows 7
- Front end : JDK 1.7 /Net beans 8.0
- Coding Language : Java
- Back End : My-SQL

V. MODULE DESCRIPTION

- ✓ Network Formation
- ✓ DHT Infrastructure Construction
- ✓ Packet Transmission
- ✓ Reputation Management

NETWORK FORMATION:

In this module the ARM selects a number of trustworthy and low-mobility nodes as reputation managers. The reputation managers constitute a locality-aware DHT, functioning as a back-bone at the center of the MANET for efficient operations of ARM.

Each normal mobile node has a watchdog to monitor and report the behaviors of its neighbors to managers.

Here, we assume that a rational user is willing to conduct neighborhood monitoring as it is willing to periodically exchange reputation information in previous reputation systems, aiming to create a trustworthy network environment.

DHT INFRASTRUCTURE CONSTRUCTION:

In this module the logical topology, the distance between nodes' IDs represents their logical distance. To build managers into a locality-aware DHT, we assign a sequence of consecutive IDs to the managers along the path connecting all nodes once in a cycle.

In a MANET, each node identifies its neighbors by sending “hello” messages. Thus, a node can infer the relative physical closeness of its neighbors by the actual communication latency.

To assign IDs to managers, we first choose a trustworthy bootstrap manager and assign it ID 0. Then, it chooses its physically closest node as its successor and assigns it ID 1. The successor finds its successor and assigns it ID 2.

The process is repeated until the bootstrap node is reached. At this time, a complete cycle is formed and all managers have been assigned numerically continuous IDs. The last node in the created path with ID must be in the transmission range of , i.e., the successor of is . Since only the physically close nodes can have sequential IDs, the constructed logical overlay topology is consistent with the physical topology of managers.

Then, each manager builds a DHT routing table containing neighbors based on a DHT neighbor determination protocol using broadcasting.

PACKET TRANSMISSION:

This module is helps to find When node n1 looks for a path for packet transmissions, it broadcasts a path query message to the packet destination. When nodes n2 and n3 receive the query, they check whether n1 is on their blacklists. If so, they ignore n1's query.

Otherwise, they respond to n1. n1 then forwards the packet along a discovered path consisting of cooperative nodes including n2 and n3. The neighbor nodes of communicating nodes and monitor the data transmission using their watchdog and report the observed transmission rate to their closest managers.

REPUTATION MANAGEMENT:

Relying on the DHT, the managers merge all reputation reports about n2 and n3, respectively, and produce their global reputations. The DHT overlay sup-ports efficient reputation information collection and querying. ARM adds credits to the accounts of n2 and n3 and decreases the account of n1. According to the reputation-adaptive account management in ARM, higher reputation leads to more earned credits for service suppliers (n2 and n3) and lower service charges for service receivers n1. If the reputations of n2 and n3 are below a threshold or n1 has a deficitaccount, managers inform all nodes in the network to put these uncooperative nodes on their blacklists.

OVERALL ARCHITECTURE DIAGRAM:

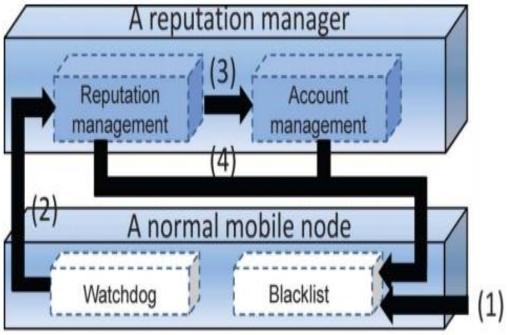


Fig 1

V.CONCLUSION

We have presented an IDS mechanism based on End-to-End connection for securing the OLSR protocol. Our mechanism can detect and isolate many types of misbehavior node(s) between the source and the destination then a blacklist of misbehavior nodes is created and broadcasting to 1-Neighbors.Accurate decisions taken by the nodes decision. Another path to destination is detected by eliminating the misbehaving nodes. We achieved better performance results when action was taken to isolate misbehavior nodes by utilizing the blacklist created and broadcasting to other nodes in the network. The simulation results showed that our mechanism is able to isolate many attackers, while keeping low overhead in terms of network traffic. Our future work will be focused on how to apply the proposed IDS on other MANET routing protocols methods.

EXPERIMENTAL SETUP:

Performance Evaluation:

The proposed design is integrated with the OLSR protocol. The Netbeans with java is used to simulate our proposed algorithm. In our simulation, 100 mobile nodes move in a 1000 meter x 1000 meter square region for 150 seconds simulation time. All the nodes have the same transmission range of 250 meters. The simulated traffic used is Constant Bit Rate (CBR) and Poisson traffic. Our simulation settings and parameters of OLSR are summarized in Table 1.1

Parameters	Values
Number of Nodes	Hundred (100)
Simulation Area	1000×1000 (m)
Sensor Node Deployment	Random Deployment
Number of Cluster Head	Two (2)
Simulation Time	150 sec
Protocol	OLSR
Battery	Initial capacity is assumed to be constant
Traffic Source	Constant Bit Rate (CBR)
Data Rate	250 kbps
Packet size	288 bits/packet or 36 Bytes
Transmission Range	250 mts
Node Ground Speed	0.5 m/s
Pause Time	5 ms
Round time	30 s

Table 1.1 Simulation Parameters

Here is the performance of analyzed by means of throughput, end-to-end delay, minimum energy consumption, packet delivery ratio and network lifetime. Here is the performance of analyzed by means of throughput, end-to-end delay, minimum energy consumption, packet delivery ratio and network lifetime.

REFERENCES:

1. S.-H. Lee, M. Gerla, H. Krawczyk, K.-W. Lee, and E. A. Quaglia, **“Quantitative evaluation of secure network coding using homomorphic signature/hashing”,** in Proc. NetCod, Beijing, China, Jul. 2011, pp. 1–10.
2. J. Joy, Y. Yu-Ting, V. Perez, D. Lu, and M. Gerla, **“A new approach to coding in content-based MANETs”,**in Proc. Int. Conf. Comput., Netw. Commun. (ICNC), Honolulu, HI, USA, Feb. 2014, pp. 173–177.
3. L. Buttyán, L. Dóra, M. Félegyházi, and I. Vajda, **“Barter trade improves message delivery in opportunistic networks”,**Ad Hoc

Netw., vol. 8, no. 1, pp. 1–14, Jan. 2010.

4. Y. Zhang and M. van der Schaar, **"Peer-to-peer multimedia sharing based on social norms",**Image Commun., vol. 27, no. 5, pp. 383–400, May 2012.
5. T. Chen, F. Wu, and S. Zhong, **"FITS: A finite-time reputation system for cooperation in wireless ad hoc networks",**IEEE Trans. Comput., vol. 60, no. 7, pp. 1045–1056, Jul. 2010.
6. T. Chen and S. Zhong, **"INPAC: An enforceable incentive scheme for wireless networks using network coding",** in Proc. IEEE INFOCOM, Mar. 2010, pp. 1828–1836.
7. C. Wu, M. Gerla, and M. van der Schaar, "Social norm incentives for secure network coding in MANETs," in Proc. IEEE NetCod, Jun. 2012, pp. 179–184.
8. J. Dong, R. Curtmola, and C. Nita-Rotaru, **"Practical defenses against pollution attacks in wireless network coding",**ACM Trans. Syst. Inf. Secur., vol. 14, no. 1, May 2011, Art.no.7