Fellowship: Defense against Flooding and Packet Drop Attacks in MANET

Venkatesan Balakrishnan Vijay Varadharajan Udaya Kiran Tupakula

***Abstract* — In this paper, we propose an obligation-based model called *fellowship* to mitigate the flooding and packet drop attacks. We also explain how the fellowship model identifies and penalizes both the malicious and selfish nodes respectively in mobile ad hoc networks (MANET). The main advantages of our model are: it unifies the framework to defend both flooding and packet drop attacks, it identifies and expels the malicious and selfish nodes that fail to contribute their resources, and rejoins the repenting malicious and selfish nodes into the network. In addition, our technique does not rely on any centralized authority or tamper-proof hardware.**

***Index Terms* — Ad-hoc networks, Wireless networks, Security, Selfish nodes, Fellowship, Cooperation, Flooding and Packet drop attacks.**

I. Introduction

Mobile ad hoc networks form on the fly anywhere and at any time due to the self-organized characteristics. They can reach any part of the network in the absence of an infrastructure through multiple hops. These networks promise more commercial prospective and advantage due to their flexibility. Nevertheless, security in ad hoc networks rests heavily on the existence of secure communication. Given the fact that the environment is not conducive to centralized trusted authority, an array of significant secure routing approaches [1-5] have been proposed to achieve secure communication. Although the proposals attain secure routing despite few fundamental challenges, they only target to secure functional ad hoc networks. For this reason, flooding and packet drop attacks that deter the availability of the network services can override the secure routing approaches.

In this paper, we show how to mitigate the flooding and packet drop attacks using our *fellowship* model. Fellowship is an obligation-based model which defends both the malicious and selfish nodes with respect to the above-mentioned attacks. The architecture comprises of three operational components -- rate-limitation component, enforcement component, and restoration component. Rate-limitation minimizes the flooding attacks, while the enforcement component reduces the packet drop attacks. The ambiguity between the intentional and accidental packet drops is resolved using the restoration component. Conceptually, the fellowship model enforces the selfish nodes in the neighborhood to obligate towards the network services. Otherwise, it identifies and isolates the malicious nodes from deriving further network services. Any selfish node that fails to obligate are excluded from the neighborhood, while the repenting malicious (or selfish) nodes are given an opportunity to rejoin the network.

Section II gives an overview of the architecture of fellowship model and section III concludes.

INSS Research Group, Department of Computing, Macquarie University, North Ryde, Sydney, NSW Australia 2109. (e-mail: venkat@ics.mq.edu.au, vijay@ics.mq.edu.au, udaya@ics.mq.edu.au).

II. Fellowship Architecture

A. Assumptions and Attacker Model

We assume that the nodes communicate using a single shared bi-directional wireless channel and all the transmissions and receptions are omni-directional. All the nodes operate in promiscuous mode and do not use any tamper proof hardware. The network may contain heterogeneous nodes with different energy levels and computational powers. The rapid growth in storage capacity eases the constraints associated with buffer requirements.

We refer to nodes that are one-hop away as *neighbors* and the region under a node's transmission range as the node's *environment*. We refer to the packet forwarding and bandwidth sharing as the *network services*. Also, we do not consider privacy issues in this paper. We expect a one-to-one mapping exists between the medium access control (MAC) addresses and Internet Protocol (IP) addresses. The adversary nodes can also modify or fabricate the packets during the routing events. We rely on the crypto-based secure routing approaches [1-5] to defend the threats and attacks related to integrity and authenticity of the packets. Hence, we inherit the assumptions from the secure routing approaches that do not violate our hypothesis. Also, we assume that the underlying crypto primitives in the secure routing approaches are secure.

We refer to nodes that disrupt the availability of network services with an intention to drain other node's resources or to prevent other node's from accessing the transmission medium as *malicious nodes*. During packet drop attacks, the *selectively misbehaving malicious node* ignores the requests received from a specific node but re-transmits other node's requests. Conversely, it can also flood the channel to block the receptions and transmissions of a specific node. In summary, we assume that the selectively misbehaving nodes which are a subset of malicious nodes to exhibit either of the above-mentioned behaviors or both in a sporadic or persistent

1-4244-0143-7/06/$20.00 ©2006 IEEE

manner.

Selfish nodes are unique to ad hoc networks because of the prevailing heterogeneity and the resource constraints among the participating nodes. These nodes remain a part of the network but exploit the self-organized characteristics to retain their resources or use their resources to override other nodes. They achieve their goal by failing to commit their resources for the requesting node, i.e. by dropping the requesting node's packet. Alternatively, the selfish nodes with relatively high resource in the environment occupy the transmission channel for forwarding self-generated packets. For this, they stay away from the medium access control layer's contention resolution mechanism and hijack the channel.

The primary motivation of the selfish nodes is to carry out their own transmissions and receptions, for which they are dependent on the network services. Thus, they may intelligently comply with any model that is proposed to mitigate the selfishness. Although the objective of the selfish nodes is distinct from the objective of malicious nodes, we suppose that the effect of selfishness will equate to the end result of maliciousness. By this, we mean both selfish and malicious nodes equally disrupt the availability of networks services. We illustrate the seriousness of packet drop attack in [9]. We refer the reader to [10] for the introduction of fellowship model concepts.

B. Overview

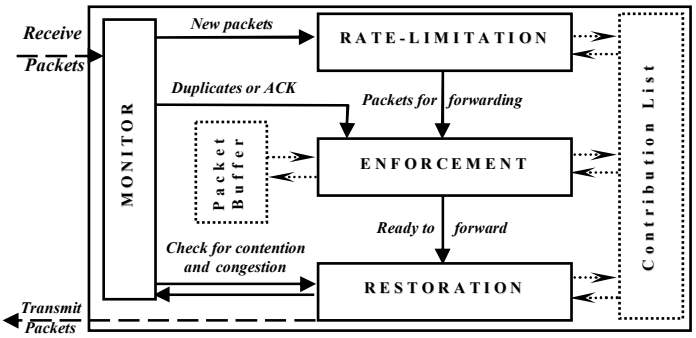

Figure 1. Architecture of the Fellowship Model

Fellowship model is invoked prior to the base routing or secure routing in terms of functionality. We assume that every participating node is *obligated* towards the network services in order to communicate with the desired node. Unlike the Nuglets [6] and Sprite [7], the obligation-based fellowship model is derived from the condition of peers sharing similar interests, ideals, experiences and goals, having heterogeneous potential resources, and wishing to participate in the network on equal terms. Unlike the incentive methods [6, 7], we measure the obligation in terms of resource commitment (for example, battery-energy). Thus there is no need to charge a node or to pay incentives. Although in a way it removes the need for an indirection such as a centralized authority or a tamper-resistant hardware, we have a distinct reason for the motivation. The cooperative approaches discussed above either increment or decrement the measurement metrics only in terms of the packets re-transmitted or dropped by the neighbors. According to our definition of selfish nodes, we envisage an intelligent selfish node to comply with the cooperative approaches but derive more resources from the neighbors. For every packet that is forwarded in favor of the neighbor, the selfish node can force the neighbor to forward larger packets in return. The service derived from forcing the neighbor to forward additional bytes may otherwise equate to the resource conserved by dropping the neighbor's packet.

Fellowship model is enforced at every node through the architecture shown in Figure 1. Each incoming packet has to pass through the three components (rate limitation, enforcement, and restoration) before being sent out. The rate-limitation component diminishes the flooding attacks with the implication that each node is obligated to share the bandwidth with the neighbors in the environment. The packet drop attack is mitigated by the enforcement component which enforces each node to obligate significant resources for being a part of the network. Whenever a node obliges to forward the request but is unable to do so due to unforeseen conditions (such as contention or congestion), the obligation is extended as liability by the restoration component. In other words, we believe that the fellowship model establishes cooperation in the network.

The cooperation is established through the operations of the monitor. It interfaces the three operational components to the medium access layer's contention resolution mechanism along with the transmission buffer's internal state. Also, it pipes the promiscuously received packets and acknowledgements to the components above. From the contention resolution mechanism and the promiscuous operation, a node can identify the neighbor's intentional packet drops and the traffic generation rate. Further on taking into account the size of transmission buffer and the availability of the medium at a given time, contention or congestion at a node can be evaluated. We treat the monitor to be the catalyst for fellowship model.

The architecture maintains two important data structures – packet-buffer and contribution-list. Recently transmitted packets are stored in the packet-buffer for future examinations. Alternatively, the signature of the packets, i.e., the headers and trailers can be stored to reduce the storage. The duration for which the packets are retained is proportional to the average time taken to complete the route discovery cycle. This is given by the base routing protocol operating above. In the case of link-error messages received from its own interface through the monitor, the corresponding packet is discarded from the packet-buffer.

At the initial stages of deployment, each node commits a significant proportion of the resource (for example, battery energy) for the network services. The committed resource is equally distributed among the 'n' nodes. When it is infeasible to estimate the total number of nodes or if there is an incremental inclusion of nodes, then the commitment can be defined for an individual node. In summary, the *contribution-list* is a tuple containing two fields – *node identity* and *contribution-count*. The contribution-count holds the resource committed to the node given by the 'node identity'. We

1-4244-0143-7/06/$20.00 ©2006 IEEE

measure the resource contributed for forwarding a neighbor's packet as the *contribution-metric 'δ'* (Table 1). It is equivalent to unity for packets whose size is pre-defined to IDEAL_SIZE. For packets of size greater or lesser than IDEAL_SIZE, the contributed resource is, 'δ' multiplied by a real number. This states that the contribution-count is the multiple of the contribution-metric (δ). For the rest of paper, we assume the size of all transmitted and received packets to be of IDEAL_SIZE (i.e. $\delta = 1$).

δ	Contribution-metric (1 for packet of IDEAL_SIZE)
θ	Merit-factor (≥ contribution-metric)
λ	Demerit-factor (≥ merit-factor)
τ	Transmission-threshold (≥MinTrans & ≤MaxTrans)

Table 1. Notations used in the Architecture

The amount of resources committed for every other node depends on the contributing node because of the heterogeneity in resources and the absence of centralized authority. Other factors affecting the commitment is the node to which the resource is contributed and the type of network, which can be managed-network or pure-network. A managed network excludes unauthorized nodes through pre-deployed keys or certificates but does not eliminate the fact that authenticated peers may be malignant. A pure network has no pre-established infrastructure and the network is created on the fly. From here onwards, we introduce and explain the architecture with respect to pure-networks. We believe that meeting the demands of pure-networks will implicitly meet the requirements of managed-networks. In the following, we introduce the operations of each component with respect to the reception end of a benign node.

Rate Limitation: *Every participating node is obligated to share the transmission channel equally with the neighbors in the environment. Nodes failing to oblige are expelled from the neighborhood by means of non-contribution.*

The rate-limitation component promiscuously monitors each requesting neighbor's channel usage at regular intervals of time. For the remaining sections, we relate the channel usage in terms of the packets generated during an interval. If the packets generated by the neighbor exceeds the *transmission-threshold (τ)* within the given interval, then the neighbor is anticipated to be malicious or selfish and the packet is discarded as a precautionary measure. Subsequently, the corresponding contribution-count for the requesting neighbor is decremented by the *demerit-factor (λ)* as a penalty. We choose 'λ' to be greater than 'δ' for violating the obligation. Note that this portrays current node's decision to withdraw the committed contribution from contribution-count, where the withdrawal is greater than the unit of contribution. The decrement operation is invoked for each packet generated thereafter within that interval. We believe that successive operations ensure the requesting neighbor to oblige. In other words, the requesting neighbor who is flooding drains the energy because the generated packet is never propagated. Nevertheless, if the requesting neighbor's channel usage is within 'τ', then the packet is passed on to the enforcement component.

We identify two design options to choose an optimum value for the transmission-threshold 'τ'. The first option is static and determined during the initial stages of the network. The value of 'τ' at each node is derived from the operational bandwidth of the transmission medium and the expected average node density per neighborhood. The latter option is dynamic and 'τ' is deduced at each node from the operational bandwidth and total number of active neighbors. The number of active neighbors is inferred from the recently received requests with new 'node identity' and failed link-layer acknowledgements. The advantage of the latter design is that the benign node with low density of neighbors can make use of the available bandwidth more efficiently than the earlier design. Otherwise, both operate in a similar way especially at high node densities. We set the range of transmission-threshold 'τ' as*: $1 \leq MinTans \leq \tau \leq MaxTrans \leq Bandwidth$.* 'MinTrans' is the minimum value of 'τ', which may equate to single packet and the maximum value of 'τ', i.e. 'MaxTrans' can be at most equivalent to the bandwidth of the channel.

Enforcement: *Every participating node is obligated to contribute a significant level of its resources for forwarding the neighbor's packets, in order to be a part of the network and to derive similar services from the corresponding neighbor's enforced obligation as reflexive contribution. The commitment for the contribution is proportional to the node's potential resources, the period it stays in network and the type of association it has with the neighbors. Alternately, detection of intentional non-contribution prevents the node from drawing similar contributions ultimately resulting in expulsion.*

The enforcement component is responsible for achieving co-operation among the participating nodes. In other words, it defends the packet drop attacks. A packet that is received from the neighbor reaches the enforcement component only if it satisfies the operations of the rate-limitation as explained above. If the contribution-count corresponding to the requesting neighbor is positive (which is supposed to be at the beginning of the network), then the enforcement component performs two actions. First, it buffers the packet (or its signature) in the packet-buffer for future reference. This assists the benign node to assert whether the next-hop neighbor is forwarding the packet or not based on the acknowledgement or promiscuous mode of operation. Second, it decreases the contribution-count corresponding to the requesting neighbor by 'δ' (i.e. 1 as a sign of contribution*)* and transfers the packet to the restoration component. Alternatively, if the contribution-count of the requesting neighbor is negative, the packet is discarded silently. The reasoning rests on the conclusion that the neighbor may be

1-4244-0143-7/06/$20.00 ©2006 IEEE

malicious or selfish.

Restoration: *Every participating node that has committed to contribute the resources for the requesting neighbor's packet but happens to drop the packet due to contention or congestion is liable to oblige a significant level of resources for the requesting neighbor's subsequent packet. Failing to extend the obligation as liability lowers the probability of gaining cooperation and ultimately results in expulsion.*

The restoration component makes the best possible effort to forward/route the packet to the next node. Prior to any transmission, it checks the transmission buffer queue to decide the congestion level. Sequentially, it investigates the Network Allocation Vector's (NAV) value [8] to understand the contention for the medium and then senses the transmission channel for availability. If the restoration component has to drop the packet due to some conditions (such as congestions or contentions), then it extends the obligation as liability towards the requesting neighbor's future packet. To reflect this, the contribution-count for the requesting neighbor at the current node is incremented by the *merit-factor (θ)*. We recommend 'θ' to be greater than 'δ' in order to reflect the benign node's liability for dropping the neighbor's packet.

It should be noted that, apart from the malicious or selfish actions, contention is likely to happen when heavy traffic is routed through the node and its environment. This is possible if the node happened to be in the zone that is centric to the network in terms of geographical location. As a result of the contention, the packets received frequently for forwarding, congests the transmission buffer resulting in overflow. The other possibilities for packet drop are as follows. The re-transmitted packets can probably collide with other's packets ending up in errors. Also, the packet may be dropped if the next-hop neighbor specified by the routing protocol cannot be reached. We preclude the last two situations from the scope of the restoration component because the fellowship model only obliges to contribute the committed resources. In both the situations – collision and broken-links, the current node has contributed its resource by forwarding the packet. Moreover, in the case of broken-links, the generation of route errors by the routing protocols to inform the previous-hop neighbor implicitly solves the issue. Furthermore, secure routing approaches can be deployed to mitigate the falsification of route errors. Hence, we consider only the contentions and congestions, where the packet is internally dropped due to non-availability of the channel or lack of resource respectively. We could have used an additional status message to inform the requesting neighbor regarding the contentions or congestions, but it leads to some issues. First, the message exchange may aggregate the contention and congestion. Second, it may also open door to other types of denial of service attacks.

Until now we have been only discussing the architecture from the perspective of a receiving node. Let us consider the situation from the perspective of a transmitting node. If the packet from node 'A' is successfully forwarded by its neighbor node 'B' to node 'C', then node 'A' increases the contribution-count of node 'B' by 'θ'. However, if node 'B' is not benign and drops the packet; then node 'B' not only fails to collect the contribution 'θ', but also loses the credentials equivalent to 'λ'. Recollect that 'λ' greater than 'θ' to reflect the penalty for violating the fellowship model and 'θ' is greater than 'δ' to reflect the appreciation for obliging the fellowship model.

III. Conclusion

In this paper we have presented a unified framework called *fellowship* model to deal with flooding and packet drop attacks that are caused by malicious and selfish nodes. We believe that fellowship model is a requirement for the formation and efficient operation of ad hoc networks. Trust or security protocols can be used over fellowship model to further enhance the efficiency of operation and improve the security in MANET.

References

[1] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne:: A Secure On-demand Routing Protocol for Ad Hoc Networks". *International Conference on Mobile Computing and Networking*, pp. 12 - 23, Atlanta, USA, 2002.

[2] S. Capkun and J.-P. Hubaux, "BISS: Building Secure Routing out of an Incomplete Set of Security Associations". *Proceedings of the 2003 ACM Workshop on Wireless Security*, pp. 21 - 29, San Diego, USA, 2003.

[3] Y.-C. Hu, A. Perrig, and D. B.Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks". *Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003)*, pp. 1976- 1986, 2003.

[4] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Rushing Attacks and Defense in Wireless Ad hoc Network Routing Protocols," *Proceedings of the 2003 ACM Workshop on Wireless Security*, pp. 30-40, San Diego, USA, 2003.

[5] P. Papadimitratos and Z. J. Haas, "Secure Routing for Mobile Ad hoc Networks". *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference*, San Antonio, TX, 2002.

[6] L. Buttyan and J. Hubaux, "Nuglets: A Virtual Currency to Stimulate Cooperation in Self-organized Ad hoc Networks". Swiss Federal Institute of Technology, Lausanne DSC/2001/001, 2001.

[7] S. Zhong, J. Chen, and Y. R. Yang, "Sprite: A Simple, Cheat-proof, Credit-based System for Mobile Ad-hoc Networks". *IEEE Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003)*, pp. 1987 - 1997, 2003.

[8] The Institute of Electrical and Electronics Engineers, "IEEE Computer Society LAN MAN Standards Committee. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std 802.11". 1997.

[9] V. Balakrishnan and V. Varadharajan, "Packet Drop Attack: A Serious Threat to Operational Mobile Ad Hoc Networks". *Proceedings of International Conference on Networks and Communication Systems (NCS 2005)*, pp 89-95, Krabi, Thailand, 2005.

[10] V. Balakrishnan and V. Varadharajan, "Fellowship in Mobile Ad hoc Networks". *Proceedings of IEEE Security & Privacy in Emerging Areas (SecureComm 2005),* Athens, Greece, 2005.