Self Healing Communities

Barrack Obuya Onduto University of Helsinki

Abstract—**Mobile ad hoc networks (MANETS) are vulnerable to routing attacks, especially attacks launched by non cooperative (selfish or compromised) network members. For instance, since packets loss is common in mobile wireless networks, the adversary can exploit this fact. It does this by hiding its malicious intents using complaint packet losses that appear to be caused by environmental reasons. Self healing communities counter these attacks. Redundancy in deployment is exploited and this is typical of most ad hoc networks.**

I. Introduction

A mobile ad hoc network (MANET) is an infrastructure less, mobile network formed by a collection of peer nodes using wireless radio. The radio broadcast medium used by MANETS makes them vulnerable to malicious attack.

Outsiders i.e. non-network members can monitor the open wireless medium to intercept legitimate traffic or to inject illegitimate traffic. Cryptographic schemes can protect the network from external attacks.

Some previously cooperative mobile nodes may turn selfish due to various reasons. The reasons include resource deprivation, or some mobile node with inadequate physical protection maybe captured and compromised. In this case purely cryptographic measures are not effective. This is because cryptographic trust is rendered to whoever owns the cryptographic keys, independent of the nodes networking behaviour.

The network must rely on non cryptographic means like intrusion detection systems (IDS) to cope with these non cooperative members. It is very hard to discriminate between losses caused by normal network and environmental conditions, and those caused by selfish and malicious behaviour.

Community based security is effective in defending ad hoc routing protocols against non cooperative nodes. The idea is to mitigate the adverse actions of selfish and malicious nodes by distributing the network services e.g. packet forwarding to a community of neighbouring nodes. Such a community is called 'self healing community'.

At the node level, service provision is untrustworthy and can be disrupted. However at the community level, the service provision becomes trustworthy even if some of the community members are selfish or malicious. The self healing services remain available and reliable if there is at least one 'good' cooperative member that can provide the needed services.

Some of the challenges in realizing self healing communities are:

1. Community creation and configuration: - a self healing community can be created and configured anywhere in a manner compatible with ad hoc routing protocols. The related process should only incur reasonably low overhead.
2. Community reconfiguration: - the self healing community must adapt to changes in the network topology and other dynamics. The impact of community members joining and leaving a community, and non cooperative nodes must be addressed.

In this paper we will present the concept of 'self healing community.' For each source-destination pair, the conventional 'per node forwarding' is replaced by the 'community forwarding' concept. A chain of self healing communities along the path will forward the packet. Where each community is compromised of multiple peer members, each of which can provide the needed service. This tolerates the presence of non cooperative nodes and stop disruptive attacks.

II. Routing Disruption

A. *On demand routing in MANET*

The 'community' concept is used to protect on demand routing. While proactive routing protocols exchange routing information even when there is no data transmission. On demand routing approach pays the cost of routing overhead only when it is needed. On demand routing protocol is composed of two parts:

1. Route discovery
2. Route maintenance

In route discovery, the source sends out a route request (RREQ) to the network when it needs a route to the destination. A neighbour either forwards the RREQ if it does not know the route to the destination, or sends back the needed routing information to the source. Upon receiving one or more RREQs, the destination sends back at least one reply (RREP) to the source. Contrary to RREQ flooding, RREP message is typically forwarded by a limited set of chosen forwarders, which are called 'RREP forwarders' or 'RREP nodes'. Various on demand routing protocols use different algorithms to process RREQ and RREP messages. The combination of RREQ and RREP processing establish a route between the source and the destination. Due to mobility and the dynamic nature of a network, an established route maybe broken at any time. On demand routing scheme use route error (RERR) notification to inform the source and the destination about the status. The source will initiate a new route discovery procedure to find new routes towards the destination. To overcome the overhead of a fresh restart from the source after each route outage, local recovery techniques are often applied. An example is using the cached routes of a neighbour.

B. RREP resource depletion

A malicious node can attempt to deplete network resource by repetitively initiating superfluous RREQ. In this attack, an attacker sends RREQ packets, which the underlying on demand routing protocol floods throughout the network. If the attacker is not a network member, cryptographic authentication can be added to RREQ packets to filter out those forged route discovery requests. However if the attacker is a compromised or selfish network member, the cryptographic countermeasures are ineffective. An RREQ rate limit approach reduces the number of RREQ packets each node is allowed to initiate.

Jiejun Kong et al introduced the concept of limiting the number of RREQ packets, without compromising routing performance. Approaching the ideal case, where a routing protocol only incurs one initial RREQ flood for each end to end connection. The community based healing significantly reduces the number of RREQ floods that each node initiates.

C. RREP packet and data packet loss

A malicious or selfish node may cause the loss of certain critical packets. In a route discovery procedure initiated by a good network member, an attacker can use some attacking mechanism to surpass other nodes with respect to the underlying routing metric. It is highly likely the attacker is selected en route. When the RREP comes back it may not forward or may forward a corrupt packet. The result is equivalent to RREQ resource depletion attack, except now the RREQ initiator is not the to blame. Also an attacker can severely degrade data delivery performance by selectively dropping data packets. Self healing approach can counter all such attackers, including non cooperative RREP forwarders and data forwarders. When an RREP or data packet is lost, the damaged route is locally healed within minimal latency.

Cryptography is an essential building block of network security. It relies on secrecy of keys, which are secret random variables maintained by each individual network member. Qualitative cryptographic algorithms ensure that any computationally bounded adversary cannot break the cryptosystem if these secret keys are not compromised. It is difficult to differentiate various packet loss scenarios e.g. to identify those cases caused by natural reasons such as channel interference, or those caused by non cooperative behaviour. A malicious sender can intentionally corrupt at least one random bit before packet transmission. It could also selectively drop some critical packets, so that its packet loss pattern appears to be random as expected.

In an on demand route discovery, a mobile node participating in RREQ forwarding may fail to forward RREP and data packets due to all kinds of reasons i.e. random mobility, selfishness or maliciousness. There is no fail safe method for loss discrimination between environmental reasons and non cooperative behaviour.

III. COMMUNITY BASED SECURE ROUTING PROTOCOL

A. Network assumptions

Jiejun Kong et al developed the routing layer community based security protocol, applicable to a broad variety of routing schemes. Backward compatibility is one of the design goals. Given an underlying on demand routing scheme, all original RREQ/RREP packet format and packet forwarding requirement are preserved in this design. This will make it possible to seamlessly integrate the community based paradigm with most existing ad hoc routing protocols. At the link layer the protocol assumes that a node can always monitor ongoing transmission even if the node itself is not the intended receiver. This requires the network interface to remain in the 'receive mode' i.e. reception mode during all transmission. This is less energy efficient compared to listening to packets directed to oneself only.

The protocol also assumes radio transmission is omni-directional, and symmetric. That is, if a node X is in transmission range of some node Y, then Y is in transmission range of node X. this can be enforced by the three way handshake in secure neighbour detection. At the physical layer, transmissions are vulnerable to jamming. In this protocol packet loss attacks are considered. Redundancy in the physical node is used to stop route disruption in a self organizing network. In a network locality there are redundant network members with high probability. These peer members will have identical capabilities and responsibilities in a community based communication. No centralized control or hierarchical control is assumed.

B Design principles

Localized and immediate self healing - When a packet forwarder is a non cooperative node that loses the packet, a localized, immediate and efficient self healing scheme to elect a substitution within minimal time. The healed path is a close approximation of the shortest path discovered by the original on demand route request. Extra self healing overheads are incurred only in the localized area around the damaged links.

Limit the frequency of flooding – Control packet flooding either network wide or limited scope, incurs tremendous energy expenses and wireless channel contention. Malicious nodes can explore this feature to deplete needed network resources. A secure routing paradigm that only requires a single initial RREQ flood per end to end connection should be realized. All this should be realized despite the unpredictable nature of the nodes due to mobility and wireless packet losses.

Explore useful information embedded in the initial RREQ floods – Secure routing schemes are not feasible if the abundant information embedded in the RREQ flood is not fully used. Critical information acquired from the initial RREQ floods, such as the neighbour hood snapshot, is useful to heal damaged on demand routes afterwards.

End to end maintenance – Due to the possible presence of malicious nodes, the intermediate forwarders cannot be trusted. Therefore the two ends of a connection should work towards maintaining the in between self healing communities whose shape degenerates due to node mobility. End to end maintenance include monitoring the end to end data delivery ratio, implementing end to end probing, maintaining fresh routes and finding new routes when the community en-route is empty because it is completely compromised.

IV. COMMUNITY BASED SECURITY (CBS)

Configuration and reconfiguration of self healing communities is the central part of community-based scheme. For each end to end connection, a chain of self healing communities along the shortest path are established to thwart route disruption. This section details how a secure community at each forwarding step is created and how the secure communities are maintained facing network dynamics and possible attacks.

A. Self healing community overview.

The concept of self healing community is based on he observation that wireless packet forwarding typically relies on more than one immediate neighbour to relay packets. Figure 1 shows the simplest case that node B relays packets from node A to node C. Typically, node B is within the intersection of node A and node C's radio range while node A and C cannot hear each other. In principle, all nodes within the 'moon' shaped intersection can relay packets from A to C. Nodes in such an intersection from the self healing community.

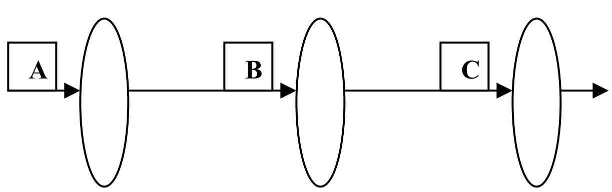

Fig 1 self healing communities as big virtual nodes

Figure 2 depicts a chain of self healing communities along a multi-hop path. Community based security explores node redundancy at each forwarding step; so that the conventional per node based forwarding scheme is seamlessly converted to a new per community based scheme. CBS does not require unusually high node redundancy. A self healing community is functional as long as there is at least one cooperative good node in the community. Intuitively, a self healing community is a big virtual node that replaces a single forwarding node in conventional routing schemes.

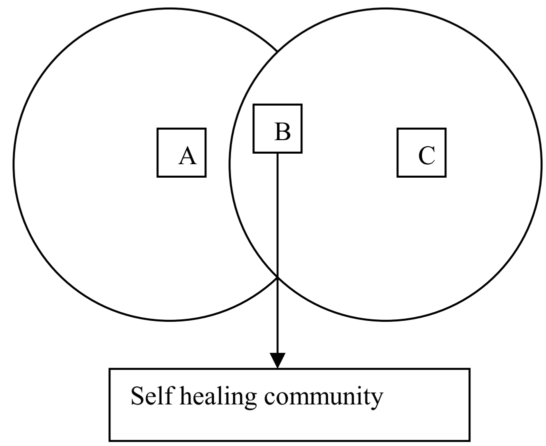

Fig 2. A self healing community between a 2 hop source and destination pair. Nodes A, B, C are the RREP forwarding nodes

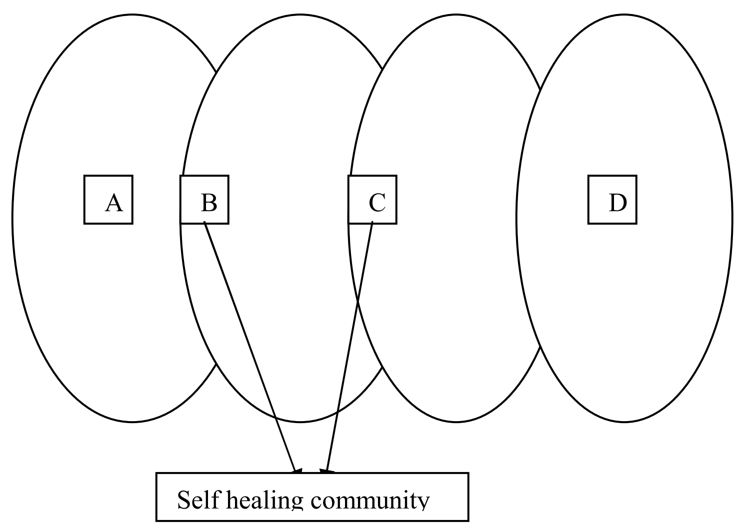

Fig 3. Packet forwarding in a self healing community along a multi hop path. Nodes A, B, C, D are the RREP forwarding nodes.

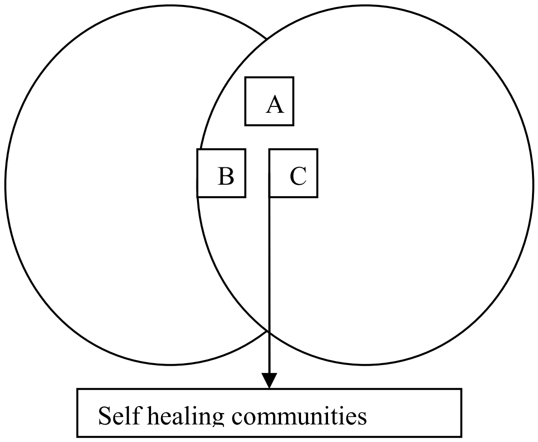

Fig 4. An inappropriate self healing community in which all the RREP forwarding nodes are within the self healing community.

B. Self healing route discovery

A self healing community must be formed properly. As a comparison to Fig 2, Fig 4 shows an inappropriate community between A and C. Because A and C are one hope neighbours, it is inefficient to introduce an extra forwarder B and pay the overhead to configure the community around B. To avoid such improper community configuration, the underlying on demand routing protocol is slightly changed. It is changed such that when B forwards its RREQ its RREQ packet, it adds its immediate upstream A in the RREQ packet.

Let's use fig 2 to describe a simple example of self healing route discovery. If B is a malicious forwarder, B can use rushing attack to make C believe that the best path between source A and destination C is through B. therefore C will unicast back an RREP packet to B. fortunately, even though the malicious B will drop the RREP packet, the other cooperative nodes in the community area will be able to identify the situation and try to take over as the forwarder.

First during RREQ phase any cooperative node Bc in the community area will already remember ***V=B*** as its one hop neighbour and ***U=A*** as V's upstream node.

Secondly during RREP phase any such cooperative Bc can detect that ***V=B*** fails to forward within a bound window. The bound window is a estimation of B's exponential back off window. If Bc is very near B and it hears all of B's reception then the initial back off window size is 32 bits, and it is doubled after every collision. However this is not always true, and some of B's reception cannot be heard by Bc due to hidden terminals. Once the estimation window expires, Bc tries to take over no matter what has happened to B, it could be selfishness, maliciousness, hidden terminals or route outage due to mobility.

Thirdly, multiple Bc nodes may compete to forward the RREP packet. Each node uses an autonomous random delay to alleviate the chances of collision. Never the less, this design does not completely eliminate take over collision. When collision occurs, the node W = A determines who wins by sending back a unicast ACK, that is, the one who is acknowledged by A. this is the one who successfully takes over.

Finally as depicted in Figure 5 below, ACK to the unicast control packet plays an important role in solving ambiguities in community configuration. At the link layer, a unicast is always acknowledged. To make the design more general, at the network layer a dedicated short ACK for RREP is implemented.

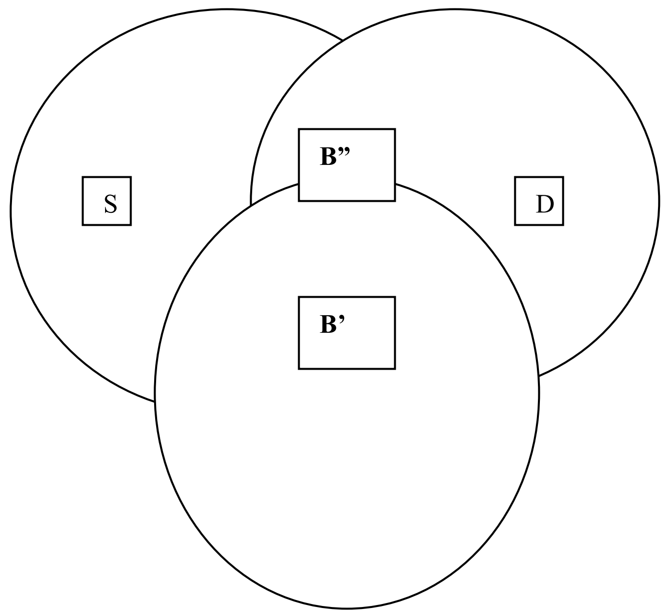

Fig 5. ACK solves ambiguity in take over collision. B” and B' (B” is not within transmission range and B' wins as forwarder

If S and D are more than two hops away, then the single-hop self healing procedure described above is executed from D to S inductively. It is guaranteed a correct RREP comes back to S if at least one cooperative node is physically present in every community area en-route.

C. Configuration of a self healing community

A chain of self healing communities is configured during the self healing RREP phase. Each node must maintain a 2-bit membership flag in its on demand soft-state for a source to destination connection. Each RREP forwarder sets its membership flag to 2. A node over-hearing three consecutive RREP ACKs sets its membership flag to 1.

This is because a self healing community member must be in the transmission range of exactly three RREP forwarders, the immediate upstream forwarder, the forwarder in the same community and the immediate downstream forwarder. As a result, a new field is added to the existing RREP packet format as given below;

RREP, <u>hop count…</u>

Where the underlined part is a counter added for the purpose of evaluating consecutiveness. The field is set to 0 by the destination D, and then increased by one by every RREP forwarder. From the three consecutive hop count values, any community member can identify the index corresponding to its own community. For example if a mobile node over hears three RREP packets for the same connection, with consecutive hop count 2, 3 and 4 in the strict order specified. Then it can conclude it is the community indexed 3.

Finally to correctly maintain the communities immediately next to the destination D, a community member only needs to hear two consecutive RREP ACKs and check whether D is involved in the packets.

D. Reconfiguration of self healing communities

The self healing communities lose shape due to mobility and other network dynamics. For each source-destination connection, end to end probing to reconfigure self healing communities is used. The probing interval is adapted with respect to network dynamics. The following intuitive example explains the essential design motives. Instead of using constrained flooding described in the example, the real end to end probing employs the self healing unicast design. Therefore the RREQ rate limit approach is practical and causes no major routing performance degradation in community based self healing.

Proactive probing by constrained flooding, an inefficient variant of community reconfiguration – suppose the two ends of a connection employ constrained RREQ floods rather than network-wide floods after RREP phase. In every constrained RREQ flood, only those nodes whose community flags for the connection are non zero i.e. set to 1 or 2, forward the RREQ packet as usual. This way, as the needed flags have set previously in RREP phase, the constrained RREQ flood only incurs forwarding overhead in the community area.

Ideally if the Tprobe is small enough, the constrained RREQ floods can maintain ad hoc routes just like network wide floods, but with much less RREQ forwarding overheads per flood. Joon Song Park et al describes how Tprobe is selected in practice following a heuristic design. A heuristic is an algorithm with provably good runtime and with optimal solution quality.

Whenever a take over action happens, the taking over node Bc sends a short report to the source S as given below;

TAKE OVER REPORT, (S, D, seq#), Bc, B

Where (S, D, seq#) identifies the end to end connection and B is the forwarding node being taken over. Bc is the nodes in the forwarding community. Tprobe is initialized to be R/v where R is the well known one hop transmission range and v is the estimated average node mobility speed.

As frequent take over action indicate more network dynamics or more non cooperative behaviour. The heuristic scheme seeks to maintain fresher self healing communities by issuing more probing requests. Meanwhile it also seeks to decrease probing overhead when the self healing communities en route are relatively stable. As a result even if the number of network wide RREQ floods for each connection is not 1, the heuristic scheme significantly reduces the network wide flooding frequency. Therefore RREQ rate limit proposal is practical in community based security.

The source S is responsible for keeping the on demand route alive because it knows whether there is further data transmission. For every Tprobe, the source S sends out a PROBE packet as given below;

PROBE, (S, D, seq#), hop_count

Upon receiving a PROBE message, the destination D replies with a PROBE REP packet as given below;

PROBE REP, (D, S, seq#), hop_count

The self healing community communities en route are reconfigured by monitoring the hop count field. A node that forwards the PROBE or PROBE REP message sets its membership flag to 2. The flag set to 2 implies the node is a forwarding member. Any node over hearing three consecutive ACKs should set its flag to 1, implying the node is a non forwarding member. The hop count is increased by 1 at each stop.

E. Self healing data delivery

Community based data delivery is a combination of conventional node based data forwarding, plus community based healing. At the source, the source node is unambiguously the current forwarder. At the intermediate stop, the most recent packet forwarder is supposed to be the current data forwarder. The current forwarder plays the role of a core in the self healing community. However if this node fails to forward a data packet due to maliciousness, selfishness, or network dynamics, members of the self healing community will make up.

V. CONCLUSION

A non cooperative network member can threaten the secure routing protocol by various means. In particular, they can deplete network resources and reduce the routing performance to minimum. These security threats have not been fully addressed in networking. Self healing communities can be used to defend against some of the security threats. Redundancy an inherent feature in ad hoc networking is deployed, to let nearby cooperative network members counter the attacks launched by the non cooperative nodes. Localized simple schemes and end to end probing is used to configure and reconfigure self healing communities. Ad hoc routes are healed locally within minimal latency. In the ideal case, only a single initial RREQ flood is needed for each end to end connection. In practice, even though this ideal case is impractical, the RREQ flooding frequency is minimized.

REFERENCES

[1] I. Aad, J.-P. Hubaux, and E. W. Knightly. Denial of Service Resilience in Ad Hoc Networks. In *ACM MOBICOM*, pages 202-215, 2004.

[2] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens. An On-Demand Secure Routing Protocol Resilient to Byzantine Failures. In *First ACM orkshop on Wireless Security (WiSe)*, pages 21-30, 2002.

[3] C. Bettstetter. Mobility Modeling in Wireless Networks: Categorization, Smooth Movement, and Border Effects. *ACM Mobile Computing and Communication Review*, 5(3):55-67, 2001.

[4] C. Bettstetter, H. Hartenstein, and X. Perez-Costa. Stochastic Properties of the Random Waypoint Mobility Model. *ACM/Kluwer Wireless Networks, Special Issue on Modeling and Analysis of Mobile Networks*, 10(5):555-567, 2004.

[5] C. Bettstetter and C. Wagner. The Spatial Node Distribution of the Random Waypoint Mobility Model. In *German Workshop on Mobile Ad Hoc Networks (WMAN)*, pages 41-58, 2002.

[6] S. Brands and D. Chaum. Distance-Bounding Pr botocols (Extended Abstract). In T. Helleseth, editor, *EUROCRYPT'93, Lecture Notes in Computer Science 765*, pages 344-359, 1993.

[7] N. Cressie. *Statistics for Spatial Data*. John Wiley and Sons, 1993