Complex Control Systems

ISSN 1310 - 8255

RELIABLE OLSR IN MANETS FOR DETECTING AND ISOLATING USER SELFISH NODES

A. Lekova [(1)], Mo Adda [(2)]

Abstract: In general Mobile Ad-hoc Networks (MANETs) deploy multi-hopping techniques to pass messages to nodes far beyond their communication ranges. Several protocols and routing algorithms have been proposed in this context. However, most of these proposals assume that nodes on their communication path are willing to relay messages to each other without obstructions. Therefore, these schemes are not immune against selfish or black-holes attacks. There are no clear rules of defense against this misbehavior, since routes in MANETs are not known in advance as the topology is highly dynamic. In this paper we propose, model, simulate and verify a variant of the Optimized Link State Routing (OLSR) protocol, named Reliable (R-OLSR) to detect and isolate selfish behavior during packet forwarding. The main contribution is the traffic monitoring in time on each multiple relay point (MRP). The abnormality in traffic patterns on MRPs in vicinity indicates for selfishness and trigger topology update in order to isolate such nodes. The proposed rules for defense are general enough to be applied to other proactive or hybrid routing protocols disseminating full or partial link state information throughout the MANETs.

Keywords: MANETs, DoS, IDS, Selfish Behavior, OLSR, UPPAAL.

1. INTRODUCTION

Mobile Ad-hoc Networks (MANETs) are spontaneous networks. They instantaneously establish communication infrastructure when it may not be present or partially destroyed. MANETs are easy to deploy and cheap to implement for short-range radios. However, mobility causes route changes continuously. Data packets must be routed via dynamic set of forwarder nodes and MANETs routing protocols are designed specifically for use in multi-hop wireless mode. Although many routing algorithms have been proposed to increase reliability of data delivery, in general they are based on contact opportunity; i.e., they implicitly assume that all nodes are willing to forward packets for others. Furthermore, since the wireless medium is shared, MANETs are completely exposed to the outsiders and there is a potential Denial of Service Attacks (DoS) [5]. Intrusion detection systems (IDS) developed for wired-networks are unsuitable for ad hoc networks with dynamic topology, since in wired-networks data monitoring is performed at data concentration points such as switches, routers and gateways [4]. IDS in MANETs require distributing services on different nodes and overcoming the

limitation of wireless medium bandwidth, transmission rates, and concerns of energy, processing and memory limitations. Different attacks affecting the performance of MANETs and some security issues are proposed in [1,4,6]. These mechanisms are not suitable for the resource constraints mobile devices, i.e., bandwidth limitation and battery power, since they results in traffic overhead for exchanging and verification of keys. The most used reactive approach is local monitoring. After unicasting data to a neighbor, the sender node overhears for a given period of time to check if the receiver node forwards the data further. Some monitoring approaches are based on the local promiscuous mode monitoring, such as 'Watchdog', 'Activity-Based Overhearing', and 'Probing'. Other rely on the employment of acknowledgments (ACKs), such as 'End-to-end AKC', '2Hop-ACK'.

The motivation of this paper is to find a distributed solution for reliable behavior of routing protocols against selfish behavior on packet forwarding overcoming the shortcomings of local monitoring schemes. Our solution is not based on acknowledgments by the destination nodes and does not depend on fixed preconfigured thresholds. Instead, we study which criteria should be analyzed to trigger topology update in order to isolate selfish or black hole nodes. These nodes are defined as shown in Fig. 1.

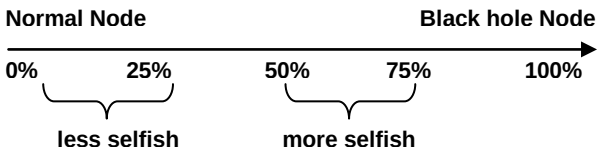

Fig. 1.. *Degree of selfishness.*

In the current MANETs, mobile nodes implement Optimized Link State Routing (OLSR) protocol [6]. The inspiration of using OLSR in you research is mainly due to the privilege roles of multiple relay points (MRP). Thus, we define clear rules for defense against selfishness on MPR nodes observing them as intermediate routers. OLSR uses topology control messages to discover and then disseminate link state information for all nodes throughout the MANETs. Individual nodes use this information to compute the path to destinations using "shortest hop" scheme. Currently, OLRS is designed to consider some degree of willingness of a node at the network layer for instance battery drain. We enhanced OLSR to consider willingness at the application layer, for instance user selfishness. A formal model in UPPAAL [2] to detect the selfish nodes in MANETs is presented and a solution how to overcome this misbehavior in routing is modeled, simulated and verified. On the basis of the results achieved from simulation and verification, a formal model of Reliable OLSR protocol (R-OLSR) is evaluated and proved to be secure against selfish nodes.

2. THE MODEL OF THE R-OLSR PROTOCOL

2.1 The concept of the R-OLSR

R-OLSR is designed and modeled to be secure against selfish nodes according to some rules for defense on MRP nodes. Each MRP monitors the sent traffic of nodes in vicinity for consecutive periods of time and isolates selfish nodes by topology update. Each sender MRP is an observer (MRP_{obs}) and checks whether the receiver MRP or 1-hop nodes (*observed*

node) forwards the data further. The MRP_{obs} starts its own chronometer (CHR_{obs}). A configurable chronometer timeout (CT_i) for each MRP_i is defined by three interval slots - s_0, s_1 and s_2. MRP_{obs} overhears the sequence number (*SN*) of sent data packets in vicinity and records their sending time as particular slot. When the MRP_{obs} overhears the packet with the same *SN*, which has been sent in the same time slot, MRP_{obs} synchronized the chronometer of the *observed node* with his own. If it is no selfish node, the forwarding delay (FD_i) is zero and the sent traffic has the same patterns in all three slots on the CHR_{obs} and CHR_i , mainly in slot 0 and 1. However, if the *observed nod*e is selfish, its chronometer is not synchronized in time and when it forwards some of the packets that happens mostly in slot 2, when the time goes over the CT_i significantly. The main idea is that the clock of a selfish MRP is synchronized with a large delay, which results in different ratio between sent traffic recorded.

The degree of selfishness (*Ds)* is estimated according to the shape of the traffic patterns. The estimated degree of selfishness $ED_s(\lambda)$ is a function of the ratio λ related to data sent in the first and last slot, as shown in equation 1

(1) $$\lambda = \text{trafficSent}[\text{MRP}_i][s_2]/\text{trafficSent}[\text{MRP}_i][s_0]$$

The results of the simulation have shown that when selfishness tends toward black holes, the ratio between data in third and first slots is bigger than certain threshold, set to 3 in this case. Then isolation of this node is imminent. When selfishness is moderate, the ratio between data in third and first slots is less or equal to certain threshold set to 2, in the simulation. Then the willingness of this node is significantly reduced. Topology update is triggered in both cases.

2.2 The Formal Model of the R-OLSR

The MANETs Node model used to evaluate the R-OLSR protocol is shown in Fig. 2. To verify the model in UPPAAL, a few assumptions were made to avoid an excess states: (1) The model consists only of 12 Node templates and only 2 of them are selfish; (2) Links were assumed to be bidirectional; (3) Topology Control is realized as global variable and represented as a connectivity matrix; (4) Unique source and destination were assumed; (5) The local monitoring scheme has been implemented only to monitor MRP nodes in vicinity.

Three types of messages are involved as structures: hello_beacon, topology_control and data_packets. Unique sequence number to each data message is deployed to ensure that a given message is not retransmitted more than once by any node. The sequence number is increased by 1 every time the message is transmitted by a sender node. The beacon period Htime, clocks x and y are used as timeout bounds for initializing phase, local and global topology discovery.

The event model generates a Boolean !INIT timeout to move all the nodes from their setup phase (START) to their beacon forward, beacon finishing and update topology (SEND_TC) states. The Node model starts in the LISTEN state and remains there unless it receives a message as of type TC, HB, internal event from the EG model or data packet. The message is only received by a node template if the connectivity matrix confirms that a link exists between the current node and sender node. The connectivity matrix (CM) defined in the global declarations is utilized to check the radio link connections between nodes for message reception. Since, wireless medium is shared all of OLSR data channels are modeled as global variables and local functions for message processing, stated in local declarations of Node

model. The channels use a global flag RadioBusy to indicate whether a channel is busy or free. This flag can be used to check if a node is allowed to broadcast a message or not. All locations where global variables have been modified are critical to be executed and modeled by urgent or committed locations. Upon receiving a HB in state REC_BEACON, the node checks if this beacon is received the first time (INIT= =true). If this guard is satisfied, the sender node is assigned as a parent of the current node model. Finally, the node model transmits HB (SEND_HELLO) using broadcast channel and moves back to the LISTEN location clearing the RadioBusy flag. A node is in the state START_DATA when it senses INT_EVENT generated by the event model. A guard about internal event - internal_invent(N_ID) is triggered when a node has a packet to send. A node broadcasts the packet to all its MRPs and remembers the sequence number (seq_numb) of every received packet to avoid cycling. After the state "LISTEN" we put the guard Buffer[N_ID].seq_numb<cur_numb. More complex procedure is adopted when data is received (DATA[N_ID]?) by a node.

To model the selfish behavior we designate a set of nodes to be selfish with certain degree. Selfish node is implemented in the model by a flag for 'Selfishness' in the upper edge after the state FLAG_ATTACK and by a number to announce its Ds, refer to figure 1. These nodes drop the packets. Wireless medium is shared, and modeled by global arrays; a global array TrafficSent keeps track of the bytes of data messages received by a MRP in the current slot. The clock zobs is reset on the transition to EVAL_TRAFFIC. The Ds is estimated by the local function eval_SentTraffic. If EDs(λ) is >3 the selfish node is excluded from connectivity matrix. If EDs(λ) is in the interval [2-3] the willingness of a node is reduced to a certain degree:

trafficSent [MRP_{obs}] [MRP_i or 1-hop node] [s]
when (SN_{MRPobs}== $SN_{MRPi\ or\ N1H}$)
if (trafficSent[MRP_i][MRP_j or 1-hop node][s_2] /
trafficSent[MRP_i][MRP_j or 1-hop node][s_0]) >2 & <3)
CASE2: hello_beacon.Willingness=WILL_NEVER
CASE3: can_hear[MRP_{obs}][MRP_i or 1-hop node]=0; //isolate selfish node
THEN updateTopology=true;

3. SIMULATION AND VERIFICATION OF THE R-OLSR

In this section we present the simulation results of figure 3 based on applying formal modeling to expose MANETs to selfish behavior. Finally, the correct work of the proposed R-OLSR protocol in UPPAAL has been verified.

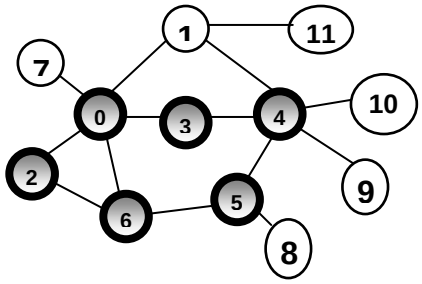

Fig. 3. *Node Model implementing R-OLSR Protocol*.

3.1 Simulation

Different number of selfish nodes with different grade of selfishness has been simulated. In Fig.4, two selfish nodes (0 and 3) with changeable Ds in the range [0-100%] affect the number of sent packets. As seen, when a selfish node has Ds = 100% the packets from Source 4 are not routed correctly by OLSR to Node 2. When the node implements R-OLSR protocol, the packets reach destination node, since R-OLSR removes selfish node from MANETs or assigns willingness of a node to WILL_NEVER and update topology by sending TC messages. Thus, nodes are informed by TC messages that Node 1 and Node 5 are current MRPs. Source 4 could send data to destination 2 via three pairs of MRPs: 3,0; 1,0; 5,6. At the beginning of the simulation nodes 0 and 3 are elected as MRPs. Then Node 3 is first detected as selfish and after topology update node 1 is elected as MRP. Then Node 0 is detected as selfish and after topology updates the path to destination goes via nodes 5 and 6.

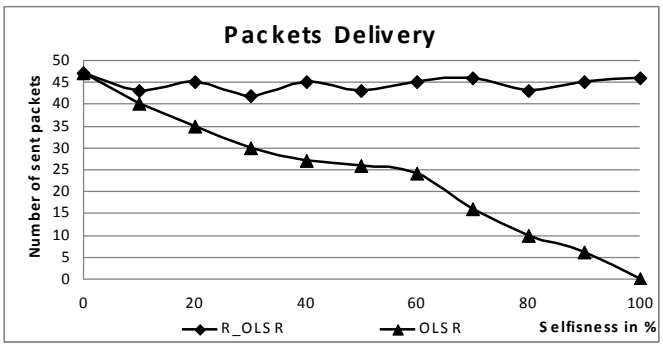

Fig. 4. *Packets Delivery*.

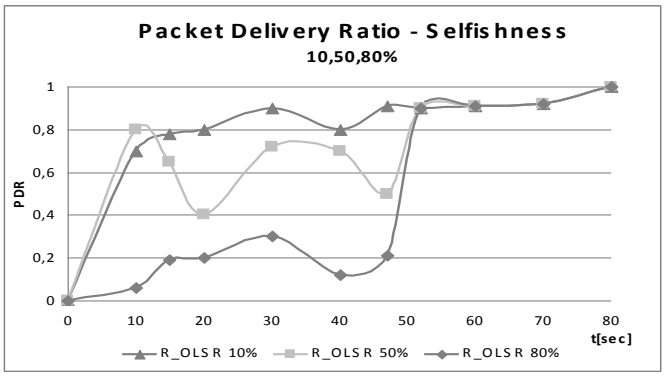

Fig. 5. *Packets Delivery Ratio*

In Fig. 5, the Packet Delivery Ratio (PDR) in function of time has been analyzed. PDR is the percentage of data packets that can be successfully delivered from the source nodes to their destination nodes. All nodes implement R-OLSR and there was one selfish node (Node 3) with three different degree of selfishness – 10, 50 and 80%. The time when the R-OLSR isolates the selfish nodes on routing corresponding to 5 steps, 10 seconds each. We found out 5 steps as enough for avoiding false detections; however 1 step also works out, but is not so robust against collisions.

3.1. Verification

The main purpose of a model-checker is to verify the model requirement specification via machine readable query language consisting of path formulae and state formulae []. State formulae describe individual states, whereas path formulae quantify over paths. Path formulae can be classified into reachability, safety and liveness.

- Reachability Properties are often used while designing a model to perform sanity checks. They ask whether a given state formula φ, eventually can be satisfied along the path, i.e., that some state satisfying φ should be reachable using the path formula E<> φ
- Safety Properties are on the form: "something will possibly never happen". For instance in a model of a communication protocol, a safety property might be: hello beaconing will always finished. In UPPAAL this is written using formula A[].
- Liveness Properties are on the form: something will eventually happen, e.g., any message that has been sent should eventually be received. In Uppaal these properties are written as $A<> \varphi$ *or* φ --> ψ

4. CONCLUSIONS

The study addresses the security of MANETs proactive routing protocol OLSR in respect of a routing service to remain stable when some nodes drop data packets and prevent data generated from the source nodes to reach the destination nodes. The main contribution of this work is formal modeling of reliable OLSR routing protocol in UPPAAL that works better in the presence of selfish or black hole nodes on packet forwarding. A novel way for isolating these nodes via triggering topology control update has been proposed. Simulations in UPPAAL showed that detection and isolation of selfish nodes doesn't introduce control overhead, time delay on packets forwarding and doesn't depend on predefined thresholds. The approach avoids false detections based on collisions and power control schemes.

The proposed clear rule for defense against selfish behavior or black hole attack is enough general and can be incorporated into other MANETs routing protocols which use designated nodes for packets forwarding, such as cluster heads or master nodes. As the future, we would like to learn about the node anomaly and derive rules for defense on MPR nodes by implementing lightweight evolving fuzzy reasoning.

REFERENCES

1 Abdalla A., I. Saroit, A. Kotb, A. Afsari, An IDS for Detecting Misbehavior Nodes in Optimized Link State Routing Protocol, Int. Journal of Advanced Computer Science, Vol. 1, No. 2, 87-91, 2011

2 Behrmann G., A. David, K. Larsen. A tutorial on uppaal. In Marco Bernardo and Flavio Corradini, editors, Formal Methods for the Design of Real-Time Systems, SFM-RT 2004, number 3185 in LNCS, pages 200-236. Springer-Verlag, 2004

3 Clausen T, P. Jacquet, A. Laouati, P. Minet, P. Muhltahler, A.Qayyum, & L. Viennot, "Optimized Link State Routing Protocol," (2003) IETF RFC 3626

4 Khokhar R., M. A. Ngadi, S. Mandala. A Review of Current Routing Attacks in Mobile Ad Hoc Networks. International Journal of Computer Science and Security (IJCSS). Volume 2, Issue 3, pp. 18-29, 2008

5 Patrikakis Ch, M. Masikos, O. Zouraraki,(2004). Distributed Denial of Service Attacks, The Internet Protocol Journal - Cisco Systems Inc, Vol. 7, N 4, pp.1-35

6 Vilela J., J. Barros, "A Cooperative Security Scheme for Optimized Link State Routing in Mobile Ad-hoc Networks," (2006) Proc of the 15th IST Mobile and Wireless Communications Summit, Greece.

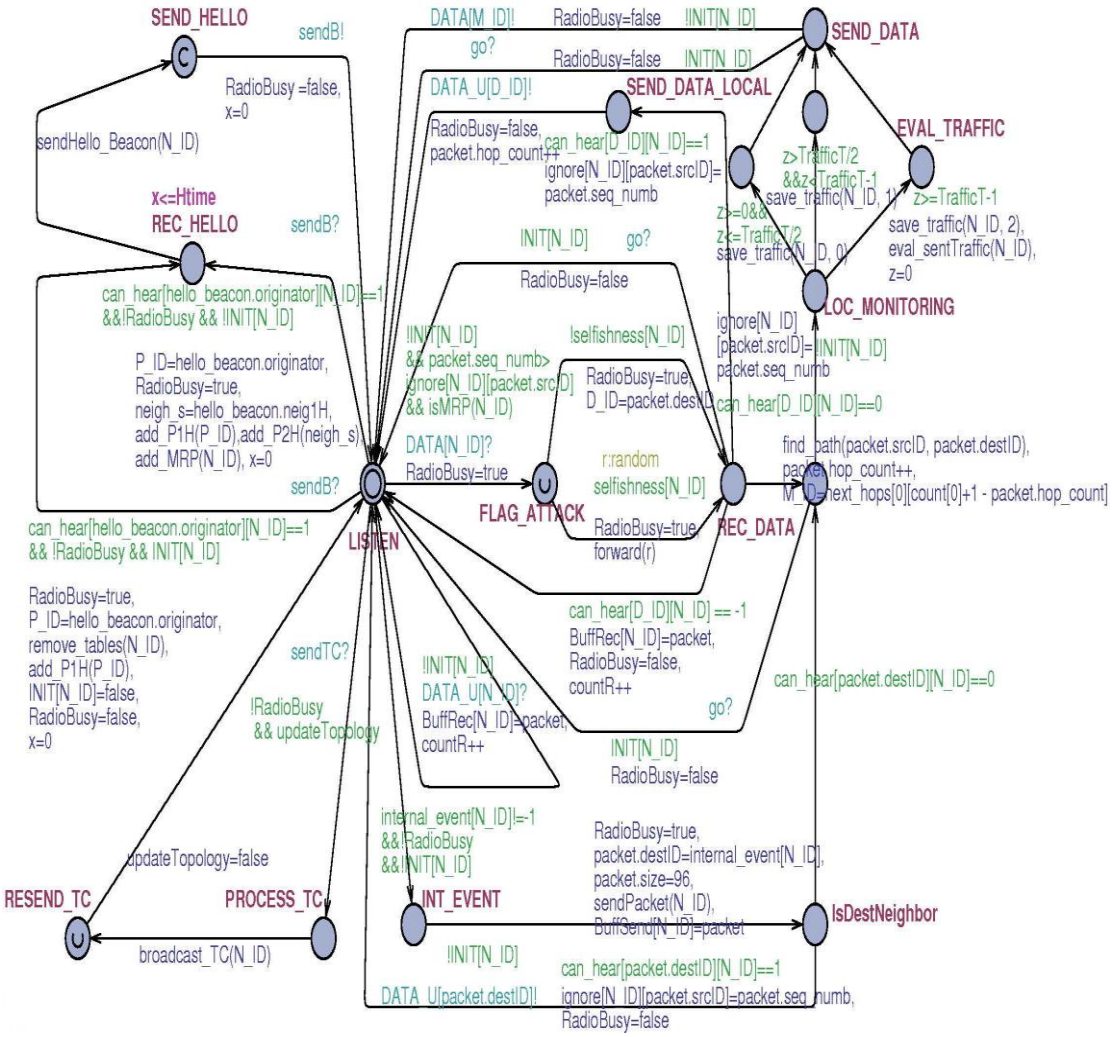

Fig. 2. *Node Model implementing R-OLSR Protocol*