ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

A Cooperative Bait Detection Approach in MANET to Detect Collaborative Attacks by Malicious Nodes

Swapnil Waghmare[1], Prof. Mininath Nigot[2]

ME.Student, Dept. of Comp.Engg. K J College of Engineering and Management Research, Pune, Maharashta, India[1]

Professor, Dept. of Comp.Engg. K J College of Engineering and Management Research, Pune, Maharashta, India[2]

ABSTRACT: In mobile ad hoc networks (MANETs), an essential requirement for the foundation of communication among nodes is that nodes should coordinate with one another. In the presence of malicious nodes, this requirement may leadserious security concerns; for instance, such node may disturb the routing process. In this context, preventing or detecting malicious nodeslaunching grayhole or collaborative blackhole in challenge. This projectattempts to determine this issue by designing a dynamic source routing (DSR)- based routing mechanism, which is referred to as the cooperative bait detection scheme(CBDS), that coordinates the advantages of both proactive and reactive defence architectures. Our CBDS system implements a reverse tracing technique to help in achieving the stated goal. Simulation results are provided, showing that in the presence of malicious-node attacks, the CBDS outperforms the DSR, 2ACK, and best-effort fault-tolerant routing (BFTR) protocols (chosen as benchmarks) in terms of packet delivery ratio and routing overhead (chosen as performance metrics).

KEYWORDS: Web mining, sequential patterns, document streams, rare events, pattern-growth, dynamic programming.

I. INTRODUCTION

Due to the widespread availability of mobile devices, mobile ad hoc networks (MANETs), have been widely used for various important applications such as military crisis operations and emergency preparedness and response operations. This is primarily due to their infrastructure less property. In a MANET, each node not only works as a host butcan also act as a router. While receiving data, nodes also need cooperation with each other to forward the data packets, thereby forming a wireless local area network. These great featuresalso come with serious drawbacks from a security point of view. Indeed, the aforementioned applications impose some stringent constraints on the security of the network topology, routing,and data traffic. For instance, the presence and collaboration of malicious nodes in the network may disrupt the routing process,leading to a malfunctioning of the network operations. Many research works have focused on the security ofMANETs. Most of them deal with prevention and detection approaches to combat individual misbehaving nodes. In thisregard, the effectiveness of these approaches becomes weak when multiple malicious nodes collude together to initiate acollaborative attack, which may result to more devastating damages to the network.

II. LITERATURE SURVEY

In [1] Dave Johnson introducedan updated version of the Dynamic Source Routing (DSR) Internet Draft (I-D) has been recently provided within the manet WG. Josh Broch began by presenting a review of the present DSR manet addressing approach. In the DSR addressing approach, a single IP address is used per node with multiple interface indexes to identify multiple interfaces. At present, a single network address space is used for all nodes in a single manet, and the potential for increasing scalability through the use of multiple manet substructureswas discussed. The chair recommended consideration for future support of subnet masking in DSR route collection. The DSR authors appeared

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

to agree that this extension was desirable and indicated it would be accommodated in a future revision. Next, Dave Maltz discussed ongoing work by CMU in providing openly available manet-related tools within the Berkeley ns2 simulation environment. This talk focused on a manet emulation capability that allows interaction of manet simulation models with live, implemented systems. This emulation capability is an exciting prospect for manet designers and developers, and will allow for easier and more comprehensive testing in the future. This emulation work leverages off initial ns2 emulation work done by Kevin Fall under the VINT project. Initial performance validation results comparing the simulation and emulation results for the existing models. The ability to introduce and evaluate real hardware and applications within the emulation environment was discussed as an additional benefit. New CMU software ports to ns2 were anticipated to be available in about 2 months.

In [2] Jiang Mingliang followed the CMU presentations by discussing an update of recent Cluster Based Routing Protocol (CBRP) modifications and evaluation results. First, a number of protocol modifications were discussed. A new local repair mechanism has been added to CBRP to improve the packet delivery ratios. A simulation of CBRP has been developed based upon existing CMU ns2 manet simulation extensions. Results showed that the CBRP improved the packet delivery ratio relative to DSR for large networks (e.g., 150-200 nodes). It was claimed that CBRP would be a good choice for scaled manet scenarios. It does not seem surprising that applying a hierarchical approach will likely improve scalability under certain scenarios. At present, these initial CBRP results need further review and interpretation by other manet participants. It is hopeful that the CBRP models will be made publicly available to the manet group for additional study and evaluation.

In [3] CharliePerkins provided an update and overview of ongoing Ad Hoc On-Demand Distance Vector (AODV) work. An updated I-D has been provided which covers improvements to the protocol with contributions from Elizabeth Royer and Samir Das. Extensions discussed included the following: service location functionality, an expanding ring search algorithm, and multicast algorithm changes. Service location extensions to AODV were discussed and were based upon RREP/RREQ indexed by protocol and port number. A long-lived association between the service and the IP address was assumed here. In addition, as an alternative to the “1-hop then infinity” searching approach presently used, a higher fidelity expanding ring search capability has been added. Questions remain regarding the best expanding ring search algorithm to use and more work is needed here. Also, a multicast modification has been added to AODV regarding the process of merging disjoint trees. Other changes are in the I-D as well, including a broadcast algorithm improvement and additional flags to improve the formation of trees. There was a WG comment questioning the rationale of doing service location in AODV vice using the Service Location Protocol (SLP). The group seemed to agree that there was general interest in mobile location protocols applied to manet and that other areas may also be of interest (e.g., anycasting)and that further discussion is needed.

In [4] the author Amir Qayyam provided an update to the OLSR protocol and discussed some initial evaluation results. A power saving modification was discussed which allows OLSR nodes to go into sleep mode. Initial simulation efforts of OLSR and a skeleton model of DSR were described. Thissimulation used an internal INRIA simulation environment to take advantage of HIPERLAN MAC layer models. A modified IMEP was developed to combine BEACON and HELLO into a single HELLO message. This was claimed to have reduced overhead within the simulations. There was no mobility in the initial simulation runs presented. A group comment questioned the present value of the results due to this lack of mobility. It was explained that these were preliminary results and that more detailed simulations would follow and that the initial framework had been developed.

In [5] author Jari Malinen provided a presentation of related ongoing manet work. They are presently working on constructing a combination of manet and mobile IP approaches for an envisioned mobile architecture. A Linux-based system implementation is being developed for evaluation. HUT is considered an approach similar to the AODV service location extensions described earlier.A number of WG manet implementers commented thatthey also have mobile IP and manet routing protocols workingtogether. More group discussion is needed here to determineif there are any unique requirements and/or solutions requiringfurther documentation.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

III. PROPOSED SYSTEM

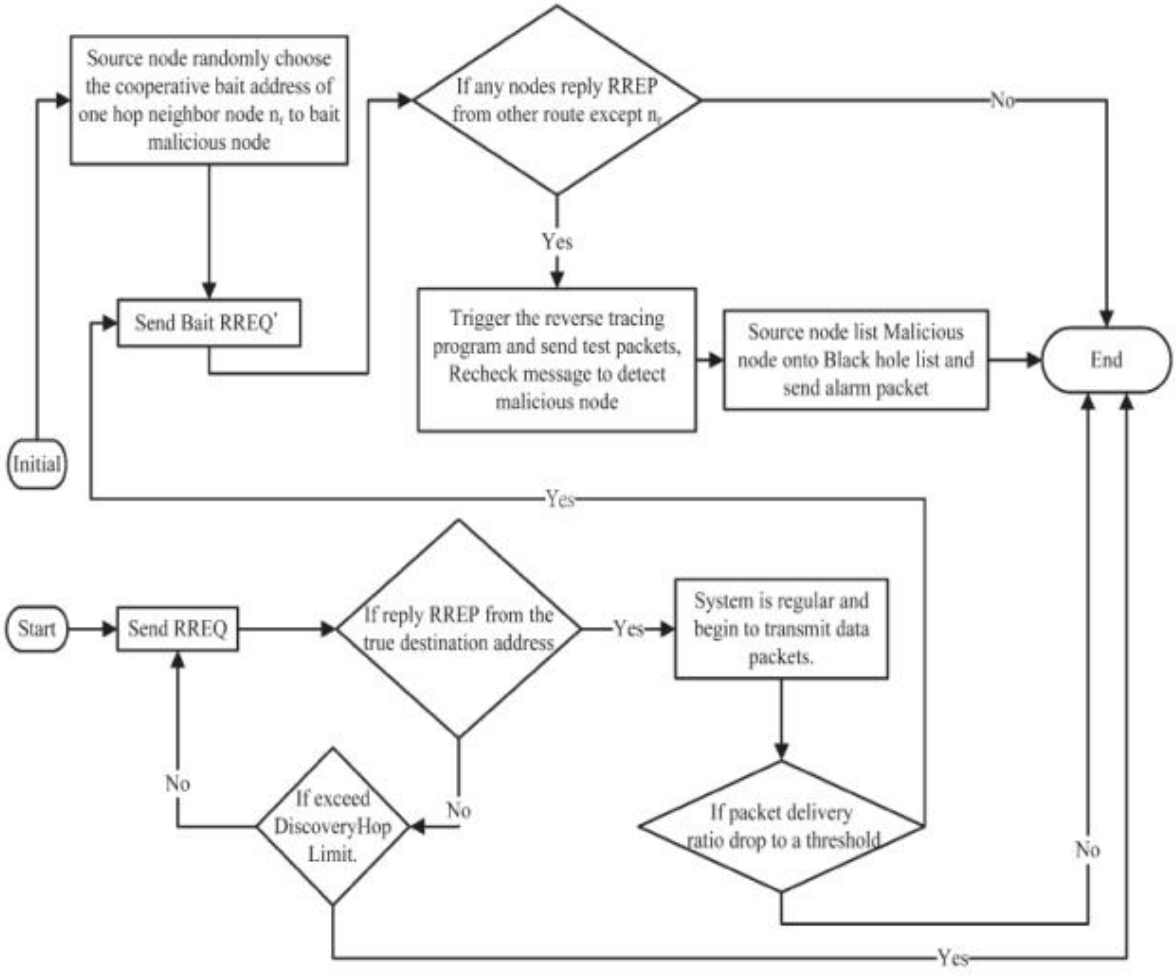
In this paper, a mechanism called "cooperative bait detection scheme" (CBDS) is presented that effectively detects the malicious nodes that attempt to launch grayhole/collaborative blackhole attacks. In our scheme, the address of an adjacent node is used as bait destination address to bait malicious nodes to send a reply RREP message, and malicious nodes are detected using a reverse tracing technique. Any detected malicious node is kept in a blackhole list so that all other nodes that participate to the routing of the message are alerted to stop communicating with any node in that list. Unlike previous works, the merit of CBDS lies in the fact that it integrates the proactive and reactive defense architectures to achieve the aforementioned goal.

ADVANTAGES OF PROPOSED SYSTEM:

- In this setting, it is assumed that when a significant drop occurs in the packet delivery ratio, an alarm is sent by the destination node back to the source node to trigger the detection mechanism again.
- This function assists in sending the bait address to entice the malicious nodes and to utilize the reverse tracing program of the CBDS to detect the exact addresses of malicious nodes.

with past techniques. In this venture our commitment is Hashtag,which will be utilized for finding the theme master.

System Architecture



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

Modules
1. Network Model.
2. Initial Bait.
3. Initial Reverse Tracing.
4. Shifted to Reactive Defense Phase.
5. Security Module.

IV. MATHEMATICAL MODEL

Let 'W' be the set of whole system which contains,
W= {RREP, RREQ', P, T, S,K,K' }.
Where,

1. RREP = Reply message.
2. RREQ' = message sent when attack occurred at some node.
3. P is the set of number of nodes in the network.
   P = {n1,…….nk,……nm,…..nr}.
4. T is set ot trusted nodes.

If node nk receives the RREP, it will separate the P list by the destination address n1 of the RREP in the IP field and get the address list,

$$Kk = \{n1, \ldots nk\}.$$

Where Kk represents the route information from source node n1 to destination node nk.
Then, node nk will determine the differences between the address list
P = {n1, . . . nk, . . . nm, . . . nr} recorded in the RREP and Kk = {n1, . . . nk}.

Consequently, we get

$$K'_k = P - K_k = \{n_{k+1}, \ldots \ldots n_m, \ldots \ldots, n_r\}$$

Where K'_krepresents the route information to the destination node (recorded after node nk).

The operation result of $K'_k$is stored in the RREP's "Reserved field" and then reverted to the source node, which would receive the RREP and the address list $K'_k$of the nodes that received the RREP.
To avoid interference by malicious nodes and to ensure that K'_kdoes not come from malicious nodes, if node nk received the RREP, it will compare the following things:

1) A. the source address in the IP fields of the RREP;
2) B. the next hop of nk in the P = {n1, . . . nk, . . . nm, . . . nr};
3) C. one hop of nk.

If A is not the same with B and C, then the received K'_kcan perform a forward back. Otherwise, nk should just forward back the K'_kthat was produced by itself.
Suppose, we assume that node n4 can reply with K'_4= {n5, n6}, n3 will check and then remove $K'_4$when it receives the RREP.
After the source node obtains the intersection set of K'_k, the dubious path information S replied by malicious nodes could be detected, i.e.,

$$S= K'_1 \cap K'_2 \cap K'_3 \ldots . \cap K'_k.$$

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

If malicious node would reply the RREP to every RREQ, nodes that are present in a route before this action happened are assumed to be trusted. The set difference operation of P and S is conducted to acquire a temporarily trusted set T, i.e.,

$$T = P - S.$$

If a single malicious node *n*4 exist in the route, the source node *n*1pretends to send a packet to the destination node *n*6. After *n*1sends the RREQ_, node *n*4 replies with a false RREP along withthe address list,

$$P = \{n1, n2, n3, n4, n5, n6\}.$$

Here, node *n*5 is a random node filled in by *n*4.
If *n*3 had receive the replied RREP by *n*4, it would separate the *P* list by the destination address *n*1 of the RREP in the IP field and get the addresslist

$$K3 = \{n1, n2, n3\}.$$

It would then conduct the set difference operation between the address lists,
P and$K3 = \{n1, n2, n3\}$ toacquire

$K'_3 = P - K_3 = \{n4, n5, n6\}$, and would reply withthe K'_3 and RREP to the source node *n*1 according to therouting information in *P*.
Likewise, *n*2 and *n*1 would performthe same operation after receiving the RREP; will obtain

$K'_2 = \{n3, n4, n5, n6\}$ and

$K'_1 = \{n2, n3, n4, n5, n6\}$, respectively;

and then will send them back to the source node for intersection i.e. ,

$$S = K'_1 \cap K'_2 \cap K'_3 = \{n4, n5, n6\},$$

Which is the dubious path information of the malicious node.

Now to calculate the source node, $P - S = T = \{n1, n2, n3\}$ to acquire a temporarilytrusted set.

if there was a single malicious node *n*4 in theroute, which responded with a false RREP and the addresslist,

$$P = \{n1, n2, n3, n5, n4, n6\}$$

then this node would havedeliberately selected a false node *n*5 in the RREP addresslist to interfere with the follow-up operation of the source node.

However, the source node would have to intersect thereceived $K'_k$to obtain

$S = K'_1 \cap K'_2 \cap K'_3 = \{n5, n4, n6\}$ and

$T = P - S = \{n1, n2, n3\}$ and request *n*2 to listen to the nodethat *n*3 might send the packets to.

if *n*5 and*n*4 were cooperative malicious nodes, we would obtain
$T = P - S = \{n1, n2, n3\}$, and *n*2 would be requested to listen towhich node *n*3 might send the packets.
Either *n*5 or *n*4 would bedetected, and their cooperation stopped.
Hence, the remainingnodes would be baited and detected.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

V. CONCLUSION

In this approach, we have proposed a new mechanism Cooperative Bait Detection Scheme(called the CBDS) for detecting malicious nodes inMANETs under gray/collaborative blackhole attacks. Theaddress of an adjacent node is used as bait destinationaddress to bait malicious nodes to send a reply RREPmessage, and malicious nodes are detected using a reversetracing technique. Any detected malicious node is kept ina blackhole list so that all other nodes that participate tothe routing of the message are alerted to stopcommunicating with any node in that list. We have observed that the CBDS outperforms the DSR, 2ACK, and BFTRschemes, chosen as benchmark schemes, in terms of routingoverhead and packet delivery ratio.Unlike previous works, the merit of CBDS lies in the factthat it integrates the proactive and reactive defensearchitectures to achieve the aforementioned goal.

As future work, we intendto 1) investigate the feasibility of adjusting our CBDS approachto address other types of collaborative attacks on MANETsand to 2) investigate the integration of the CBDS with otherwell-known message security schemes in order to construct acomprehensive secure routing framework to protect MANETsagainst miscreants.

REFERENCES

1. Johnson, David B., David A. Maltz, and Josh Broch. "DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks." Ad hoc networking 5 (2001): 139-172.
2. Jiang, Mingliang. "Cluster based routing protocol,(CBRP)." draft-ietf-manet-cbrp-spec-01. txt, Internet draft (1999).
3. Royer, Elizabeth M., and Charles E. Perkins. "Multicast operation of the ad-hoc on-demand distance vector routing protocol." Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking. ACM, 1999.
4. Khan, Imran, and Amir Qayyum. "Performance evaluation of AODV and OLSR in highly fading vehicular ad hoc network environments." Multitopic Conference, 2009. INMIC 2009. IEEE 13th International. IEEE, 2009.
5. Perkins, Charles E., et al. "Internet connectivity for mobile ad hoc networks." Wireless Communications and Mobile Computing 2.5 (2002): 465-482.
6. C. Chang, Y.Wang, and H. Chao, “An efficientMesh-based core multicast routing protocol onMANETs,” *J. Internet Technol.*, vol. 8, no. 2, pp. 229– 239, Apr. 2007.
7. D. Johnson and D. Maltz, “Dynamic source routing in ad hoc wireless networks,” *Mobile Comput.*, pp. 153–181, 1996.
8. I. Rubin, A. Behzad, R. Zhang, H. Luo, and E. Caballero, “TBONE: A mobile-backbone protocol for ad hoc wireless networks,” in *Proc. IEEE Aerosp. Conf.*, 2002, vol. 6, pp. 2727–2740.
9. A. Baadache and A. Belmehdi, “Avoiding blackhole and cooperative blackhole attacks in wireless ad hoc networks,” *Intl. J. Comput. Sci. Inf. Security*, vol. 7, no. 1, 2010.
10. S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” in *Proc. 6th Annu. Intl. Conf. MobiCom*, 2000, pp. 255–265.
11. K. Vishnu and A. J Paul, “Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks,” *Int. J. Comput. Appl.*, vol. 1, no. 22, pp. 28–32, 2010.