International Journal Of Engineering Research & Management Technology

ISSN: 2348-4039

IJERMT

Email: editor@ijermt.org MaY- 2014 Volume 1, Issue Website: ijermt.org

Nature Based Trust Security Protocol against Greyhole Attacks in Opportunistic Networks

Dr K.K. Saini
Director, Ganga Technical Campus, Bhadurgarh, Haryana, India

Aakanksha Saini
Division of Information Technology
Netaji Subhas Institute of Technology
University of Delhi, Delhi, India

Mehak
Research Scholer

Abstract:
Opportunistic network is a type of wireless network that provides the opportunity to interact and transfer information between spontaneous mobile nodes. In this network one of the most important issues is the selection of the best intermediate hop to forward the message to the destination i.e. routing, because almost nil pre-requisite knowledge is given about the network. This paper presents a trust framework for opportunistic network against greyhole attack. Here the greyhole nodes are divided into three groups according to their nature (probability) of behaving like a blackhole. The selection of next hop to forward the data packets is based on the trust value calculated and analyzed at each sender node. The effectiveness of the proposed Nature Based Trust (NBT) Security Protocol is shown using One simulator.

I. INTRODUCTION

Opportunistic network (Oppnet) is a subclass of Delay-Tolerant Network. As communication opportunities are few and episodic, an end-to-end path between the source and the destination may never exist. The nodes can communicate with each other via all types of communication media like Bluetooth [1], WiFi [2], and other communication-based technologies and point of access towards the fixed Internet or a satellite [3]. In times of war where network becomes sparse or in rural areas where there is restrained access to internet, normal TCP/IP protocol will not work properly. Oppnets are the best solution there. Routing is the most compelling challenge in Oppnets. Routing of messages in Oppnets is based on the contact opportunity between the nodes that arises due to their mobility, Store-Carry-and-Forward technique and the local forwarding between the nodes [4, 5]. The design of efficient routing strategies for opportunistic networks is generally a complicated task due to the absence of knowledge about the topological evolution of the network. Even if an appropriate routing methodology is chosen, it is hard to know whether a candidate node behaves appropriately or malevolently in the system. To know the malevolent behavior of nodes in the network some techniques are required that let the routing node knows the demeanor of other nodes through exchange and calculation of certain social parameters. This helps in identifying the malevolent behavior of nodes in the network. A malicious behavior leads to a considerable delay in the message delivery or no delivery at all in the network under consideration [6]. This paper secures the network from greyhole attack through the proposed NBT Security protocol.

A greyhole attack is an attack, where at one moment of time, a node advertises itself as honest, and attempts to provide faked information to attract and stop the message packets, preventing them from reaching their destinations (i.e. behaves like a blackhole node) and the same node at other moment of time behaves like a normal forwarding node.

The rest of the paper is organized as follows. Section II, the proposed Nature Based Trust Security Protocol (NBT) is described. In Section III, the simulation results are presented. Finally, Section VI concludes the work.

II. PROPOSED NATURE BASED TRUST SECURITY PROTOCOL

In this section, the protocol is introduced in detail. When a node carrying a message comes in contact with the neighboring nodes, Trust Values of neighboring nodes are checked. A threshold trust is set, nodes having higher Trust Values than threshold trust will be chosen for forwarding messages. Trust is calculated using three factors: NatureID, Latest Nature and Friend List. These factors are described below.

(i) NatureID

Nodes in the network are divided into three groups according to their nature i.e. Extrovert, Ambivert and Introvert. The nature of the node is according to their capability to become black node i.e. nodes which forward message most of the time and have less probability of becoming black hole nodes are labeled as Extrovert nodes ,and nodes which behave like black hole nodes most of the time and forward less messages are labeled as Introvert nodes. Nodes which have mediocre behavior are labeled as Ambivert nodes. An individual group is assigned with a priority number called NatureID. In the current work these values are static and arbitrarily chosen at appropriate intervals.

In real life also, Extrovert people talks and interacts more, in the same way Extrovert nodes are more interactive and forward messages in higher ratio where as Introvert nodes are less interactive and forward messages in small ratio. Performance of Ambivert nodes are in between Extrovert and Introvert nodes.

(In simulation, NatureID of Extrovert node is taken as 3, of Ambivert node is taken as 2 and of Introvert node is taken as 1)

(ii) Latest Nature

As grey nodes in the network are continuously changing their behavior from black hole node to honest node, checking their latest nature can give us some important information about their current behavior. As the messages in the network are forwarded, they store the hop IDs of the nodes through which they passed through. This gives assurance that these hops were behaving like honest node at some period of time.

In the simulation, as the node gets a message, it extracts the message details and checks the hops through which the message has passed through and the time at which they passed through. Message structure is shown below.

Message structure: This is the set $\{S_{id}, D_{id}$, Message text, V$\}$, where S_{id} is source ID, D_{id} is destination ID, V is the vector composed of the IDs of intermediate nodes between the source and the destination ,and the time at which the message is received at each intermediate node respectively. V is initially set to Ø.

The structure of V=<< (N_1, T_1), (N_2, T_2)… (N_i,T_i) …(N_m,T_m)>>, where N_i is the node's hop ID, T_i is the receiving time and $i \epsilon [1, m]$.

Each node in the network maintains a table called *Path_Route* table, in which it stores the intermediate hops extracted from the messages and the corresponding receiving time of the messages at intermediate nodes. As the nodes come in contact with each other they exchange their *Path_Route* table. So that information can be circulated. Structure of *Path_Route* table is given in Table 1.

This table shows the intermediate nodes that have forwarded messages hence behaved like white nodes at some period of time. Therefore this gives assurance that these nodes behaved like white nodes. The node that carries the message, searches for the neighboring node in this table and checks the corresponding time stamp. If the difference between current time and the time stamp is less than 20 seconds, we set *LatestWhitening_Factor* as 1, otherwise 0. In this way, latest honest nodes are selected.

Table 1: Path_Route table

Host ID	Time(in sec)
N1	23.00
N2	56.01
R1	12.21
R3	65.23

(iii) Friend List

Like humans have friend circle with whom they interact most of the time, nodes also have groups of nodes with which they interact often. As one is known by the company he keeps, similarly what type of nodes a node meet is also an important factor.

During the simulation, as the node moves it stores the HostIDs of the nodes with which it comes in contact, in its Friend_List. The structure of Friend_List is shown below:

Friend_List=<<N_1, N_2, N_3…, N_i …N_m>>, where N_i is the node's hop ID and $i \epsilon [1, m]$.

When the node carrying message comes in contact with the neighboring node, it checks in the Friend_List of neighboring node and counts number of friends it has that are Extroverts, Ambiverts and Introverts. Greater the number of Extrovert friends, better it will be for message carrying and lesser the number of Introvert friends, better it will be. Therefore, weightage is given according to the type of friends.

Therefore, Friend_Sum = U_1 *(1-1/Ex) + U_2 *(1-1/Am) + U_3*(1-1/In)

Where, U_1, U_2 and U_3 are weightages. Ex stands for number of Extrovert friends, Am stands for number of Ambivert friends and In stands for number of Introvert friends.(In our simulation, they are taken as 0.6, 0.3 and 0.1 respectively.)

(In case, any one i.e. Ex, Am or In equals to 0, 1.0 value is taken and in case Ex, Am or In equals to 1, 1.01 value is taken)

Finally, Trust Value is calculated using equation given below,

Trust_Value=NatureID+
LatestWitening_Factor+Friend_Sum

(Threshold value of Trust in this simulation is taken as 3.0.)

Figure1 shows the example of a network scenario:

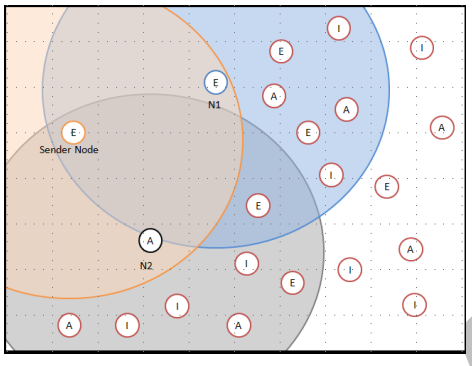


Figure 1: Example Scenario

In the figure above, nature of the respective node is indicated in the circle. E stands for Extrovert, A stands for Ambivert and I stands for Introvert. The big colored translucent circles are transmission ranges of respective nodes. Suppose at some simulation time, Sender node as shown in figure has to send the data packet to its neighboring node. It has two neighboring nodes N1 and N2 in its reach (for convenience and clarity we have taken only two options). Therefore, Trust is calculated using above described three factors. *NatureID* of N1 will be 3 and of N2 will be 2. Suppose *LatestWhitening_Factor* of N1 is 1 and that of N2 is 0 (i.e. N1 has latest entry in *Path_Route* table of Sender node and N2 doesn't have). Now,

Friend_Sum of N1 = 0.6*(1-1/3) + 0.3*(1-1/2) + 0.1*(1-1/2) = 0.6

Friend_Sum of N2 = 0.6*(1-1/2) + 0.3(1 – 1/2) + 0.1(1-1/3) = 0.516

Final *Trust_Value* of N1 = 3+1+0.6=4.6 and Final *Trust_Value* of N2 = 2+0+0.516=2.516

As *Trust_Value* of N1 is greater than 3, N1 is chosen for message forwarding.

III. SIMULATION SETUP AND RESULTS

Simulation studies have been conducted using the ONE simulator [7], to compare the effectiveness of Nature based Trust secured protocol (NBT) implemented over Epidemic router [8] under greyhole attack against the Epidemic protocol with no security under greyhole attack (let us say EGH).

A. Simulation Setup

In our simulation, a node can behave like a black node or like an honest node at any period of time. Messages are generated at honest nodes at any period of time. It is assumed that the buffer size and transmission duration of a node are limited. The simulation parameters are:

Area: 5000 m * 5000 m

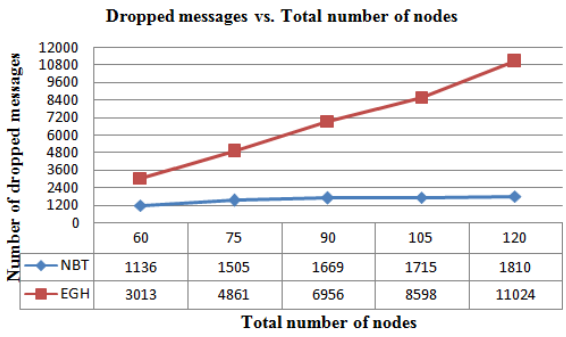
Data transfer rate: 250Kbps

Number of Groups: 3

Buffer space of each node: 50Mb
Speed range: 0.5-1.5 m/s
Wait time range: 0-120 s
Message size: 500Kb to 1Mb
Message generation interval: 25-35 s
Simulation time: 20000s
Movement Model: ShortestPathMapBasedMovement [9]
The following performance metrics are considered:
1) Dropped Message: the number of messages dropped from the buffers of the nodes.
2) Overhead Ratio: (number of relayed packets – number of delivered packets) / number of delivered packets, which is a form an assessment of the bandwidth efficiency.
3) Aborted Message: this represents the number of aborted transmissions that have occurred between nodes.
4) Delivery Probability: The probability of the messages that are correctly received by the destination within a given time period.

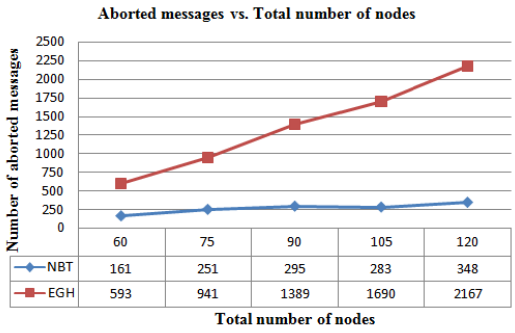
B. Simulation Results

Figures 2(a) to 2(d) show the performance of NBT Security Protocol at various Performance metrics at different number of nodes.



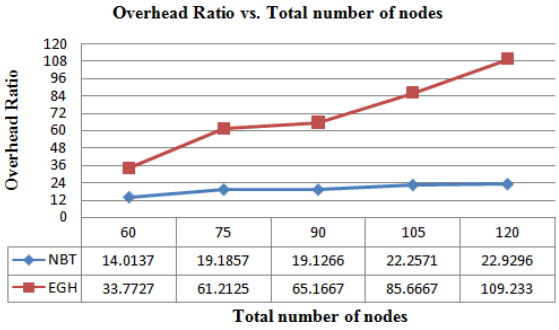
2(a)

First, total number of nodes is varied in the network and the impact of this variation is observed on the number of messages dropped from buffers of the nodes. The result is shown in Fig. 2(a). From Fig. 2(a), it can be seen that the number of messages dropped is significantly lower in case of NBT when compared with EGH. As NBT filters out and leaves the low trusted nodes.



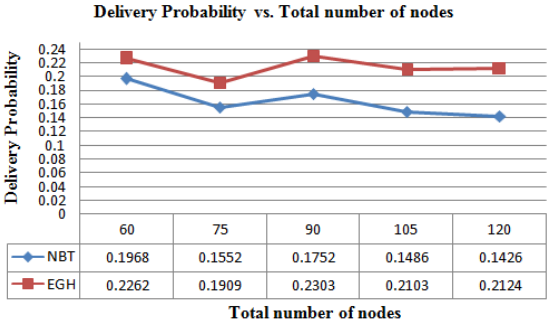
2(b)

In Fig. 2(b), as the number of nodes increase, the messages aborted is fairy less in case of NBT when compared with EGH. Aborted messages are incomplete transferred messages that waste the network resources like battery, bandwidth, etc. and which are of no use in the network



2(c)

In Fig. 2(c), it can be observed that when total number of nodes increase, the generated overhead ratio is significantly lower when using NBT compared to when using EGH. This is due to the fact that in the EGH method, there is no bound on generation of messages. Therefore, the transmissions of extra messages lead to the wastage of bandwidth. In the NBT method, nodes that have higher probability to become black nodes and have poor Friend_Lists are identified and then rejected, which prevent the above transmissions from happening, hence some bandwidths are protected.



2(d)

Figure 2: Performance Metrics vs. Total number of nodes

From Fig. 2(d) it can be observed that when the total number of nodes increases, the delivery probability values obtained when using NBT are lower compared to that observed when using EGH. This might be due to the fact that in the NBT, less trusted nodes may also include nodes with higher probabilities to deliver messages and which are rejected for the message transmission.

V. CONCLUSION

Nature Based Trust (NBT) Security Protocol is proposed to extenuate greyhole attacks in Opportunistic Networks that use Epidemic routing protocol. NBT is compared against the Epidemic protocol with no security under greyhole attack (EGH scheme). Simulation results concluded following points: (1) NBT substantially improves NBT message drop ratio compared with EGH; (2) NBT's overhead ratio is significantly lower than that of EGH; (3) the nodes' delivery probabilities in case of NBT is lower than that of EGH. These results show that NBT scheme significantly helps in reducing the usage of bandwidth of the network by limiting the extra messages that would have been sent to the blackhole nodes.

IV. REFERENCES

[1] Bluetooth, The Bluetooth Specification, http://www.bluetooth.com/Pages/Bluetooth-Home.aspx.

[2] WiFi, http://www.wifinotes.com.

[3] Sanjay Kumar Dhurandher, Deepak Kumar Sharma and Isaac Woungang, "Energy-based Performance Evaluation of Various Routing Protocols in Infrastructure-less Opportunistic Networks", in Journal of Internet Services and Information Security, volume 3.

[4] L-J. Chen, C. Hung Yu, C. Tseng, H. Chu, and C. Chou, "A Content-Centric Framework for effective Data Dissemination in Opportunistic networks", IEEE Journal on selected Areas in Communications, vol: 26, Issue: 5, June 2008, pp. 761-772.

[5] S. K. Dhurandher, D. K. Sharma, I. Woungang, and H.C. Chao, "Performance Evaluation of Various Routing Protocols in Opportunistic Networks", in Proceedings of IEEE GLOBECOM Workshop 2011**,** Houston, Texas, USA , 5-9 December, 2011, pp. 1067-1071.

[6] Sahil Gupta, Isaac Woungang, Sanjay Kumar Dhurandher, Arun Kumar and Mohammed S. Obaidat, "Trust-Based Security Protocol Against Blackhole Attacks in Opportunistic Networks" in Wireless and Mobile Computing, Networking and Communications, 2013 IEEE 9th International Conference.

[7] A. Keranen. "Opportunistic Network Environment Simulator". Special Assignment Report, Helsinki University of Technology, Dept. of Communications and Networking, May 2008.

[8] A. Demers, D. Greene, C. Hauser, W. Irish, J. Larson, S. Shenker, H. Sturgis, D. Swinehart, and D. Terry. Epidemic Algorithms for Replicated Database Maintenance. In Proceedings of the Sixth Symposium on Principles of Distributed Computing, pages 1–12, August 1987.

[9] A. Keranen, J. Andott. "Opportunistic increasing reality for DTN protocol simulations". Special Technical Report, Helsinki University of Technology, Networking Laboratory, July 2007.