www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 12 December, 2015 Page No. 15246-15251

Performance Analysis in Dynamic Social Networks

[1]Sonia Kumari, [2] Pratibha Yadav, [3] Manvendra Yadav

[1, 2]Shyama Prasad Mukherji College (For Women), University Of Delhi, India

[3]Atma Ram Sanatan Dharma College , University Of Delhi , India

[1]soniakumari.ducs@gmail.com, [2]pratibhamcadu2011@gmail.com, [3]ymanvendra@gmail.com

ABSTRACT

Social network can be generally defined as a group of individuals who are connected by a set of relationships. A key characteristic of social networks is their continual change. However, the bulk of the analysis methods developed and popularized in the field of computer were static in that all information about the time that social interactions take place is discarded. Although recently there is some work on dynamic social network analysis. In this article we have presented the overview of dynamic social grouping algorithm[10][11] . Probabilities and social behaviour are two common criteria used to route a message in disruption/delay tolerant network wherein there is only intermittent connectivity between the nodes. In this article we first discuss how the characteristics of these routing algorithms can be exploited by a malicious node to attract data packets and then dropping them to degrade the network performance. We then show the impact of such a behaviour called blackhole attack on DSG as it leverages both the social behaviour as well as the delivery probabilities to make the forwarding decisions. We present three solutions to mitigate black hole attacks. The first algorithm mitigates non collaborating blackhole nodes. In the second algorithm, we present a solution that handles collaborating blackhole nodes. The first two algorithms handle only the external attacks. It does not handle the scenario in which a node that is good initially and becomes malicious or selfish later. Finally, we present our third algorithm which handles collaborative black holes as well as internal attacks. We validate the performance of our algorithms through extensive simulation in ONE simulator.

Keywords
Security, Dynamic Social grouping (DSG), Blackholes.

1. INTRODUCTION

Routing algorithms are more effective when they rely on information regarding the contact patterns of nodes. In Social routing , the nodes assigned to the same social network will regularly interact with members of that social group. Once these groups are identified, consistent routes to nodes are recognized based on the delivery history of a group or node as in Dynamic Social Grouping(DSG)[10][11]. In these routing algorithms, Security issues become more challenging in the network due to its dynamic nature which allows any node to freely join as well as leave the network without having a physical address or getting permission[8]. Here we have discussed the black hole problem. It occurs when a malicious node referred as black hole joins the network. The black hole conducts its malicious behaviour during the process of route discovery. We present the characteristics of DSG and explain how a blackhole can use quality of DSG (i.e. by increasing group probability by increasing contact strength and by showing false value individual probability) to attract data packets and then dropping them and hence degrading the performance of network .We here discusses the three algorithms for detection and handling the blackhole . The simulation results of the proposed algorithm shows significant improvement.

2. Implementing DSG

This routing algorithm forms social groups, these groups indicate a node's regular contact patterns. The nodes initially have no awareness of their environment. A probabilistic routing schema is used to find which social groups have consistent contact with the base station. So that, these groups can be used for routing the messages to the base station. DSG Routing is based on two types of probabilities:

- Individual probability : It is the node's probability of delivering the message to the base station. Initially all the nodes are assigned the same probability, σ. The base station is given a probability of 1. Each node maintains a variable(data type: double) to store its individual probability[6].
- Group probability : It is the average of the individual probabilities[6] of all the nodes in the group. Each node calculates its group probability, depicted as β, independently, based on its contact patterns. This means that each node will have different values for the probability of the same group, based on the subset of the group which each node contacts.

The current group probability is used for the probabilities of the nodes which are the members of the group and have not been encountered yet. Let two nodes $Node_A$, $Node_B$ belonging to the same group($Group_Y$) contact each other. If the σ for all other nodes in $Group_Y$ are unknown, they are assumed to be the current β_Y . The node then calculates the average probability[6] of all members of the group, based on previous β_Y , σ_A, and σ_B, as follows:

$$\beta_Y = \sigma_A+\sigma_B + \beta_Y X(|Group_Y| - 2)/|GroupY|$$

The contact patterns of nodes are used to identify nodes which frequently contact each other, these nodes form a group. The groups formed are used to deliver messages to the base station. Identifying social groups Contact strength[7] is done by The first step in forming social groups is to calculate the contact frequency of two nodes with one another. Contact frequency[7][8] of two nodes is represented by $\lambda_{i,j}$. Initially, the contact strength is 0 between all nodes. When nodes contact each other, it is updated as follow:

$$\lambda_{A,B} = (1-\phi)\, \lambda_{a,b} + \phi/(time_{curr}-time_{pre})$$

Where,
$\lambda_{A,B}$= new contact strength
$\lambda_{a,b}$ = previous contact strength
ϕ is used to determine how much new $\lambda_{A,B}$ is based on previous contact
strength.
$time_{curr}$= current time
$time_{pre}$= time of previous contact

3. Attack Model

The blackhole is a malicious node that provide false information to other nodes that it comes in contact with and attract packets from them. After receiving these forwarded packets, Once the data is received by the black hole, it is dropped instead of being sent to the desired destination[2] . A black hole node does not generate any messages in the network and also avoid sending any message to any other node in the network. It is trying to get all messages from other nodes by showing its high individual probability and contact strength in DSG, A misbehaving blackhole carrier may show falsely large value of delivery probability or comes in contact with nodes much frequently and increases contact strength.

- In these algorithm a blackhole node as a node which announces $\lambda_{\mathbf{Bh}} = 1$ and attracts all the data packets of node in contact where $\lambda_{\mathbf{Bh}}$ is node's contact strength with destination. When a node say $Node_{Bh}$ contacts $Node_{\mathbf{B}}$ very frequently and for long duration so that it's contact strength λ_{BhB} becomes greater than a threshold and a group is formed between them. Now suppose $Node_B$ and $Node_{Bh}$ have group probabiltiy as β_{BhB} then if $\beta_{BhB} > \beta_A$ then $Node_A$ Transmit messages to $Node_{Bh}$.
- For example consider the scenario where in two nodes $Node_A$ and $Node_{Bh}$ having delivery of probability σ_A and σ_{Bh} respectively then if $\sigma_{Bh} > \sigma_A$ then $Node_A$ Transmit messages to $Node_{Bh}$.
- In this way, the other nodes tend to choose such a carrier with high probability and forward their messages to it and this malacious node drops all the messages and hence degrades the transmission performance of DTN networks [5].

Greyhole is blackhole node whose behaviour is not fixed from the begining .It sometimes behaves like a good node or sometime time behaves like a blackhole node in the network. We define internal attack as a blackhole node as a node, which is good node initially, means it forwards data packet but after some time it gets compromised and stops forwarding the data packets. It behaves like a blackhole node and presents its false information to attract data packets.

4. Algorithms for handling Blackhole and Greyhole

Our aim is to Avoid giving messages to a blackhole node. The proposed algorithm handles external attacks when a node is either good or bad i.e once a node has been announced as good it remains good. To handle malicious nodes, we propose an algorithm in which we assume presence of a trusted entity called base-station (B0). We present two approaches to handle blackhole node in DSG.

4.1 First approach

When a node transfers any message to base-station, the base station considers that node as good node and stores this information. When other node comes in contact with base-station later, they learn from the base station about all the good nodes present in the network. We propose all nodes act as a watchdog for other nodes, for example, when two nodes come in contact with each other, they first check trust information for each other. If they found that node in contact is a good node, they exchange information about all other good nodes. This approach is good in handling multiple collaborating black nodes but suffers from little long delays.

4.2 Second approach

This approach is similar to first approach, a node is considered as good if it transfers messages to base-station. When base station receives a message from any node it considers as good and stores the information. To spread the trust level information fast we do not restrict other nodes to exchange their information only if they are good for each other. We propose nodes to exchange information about other

Good nodes present in the network but we restrict to exchange their own trust level as good with each other. i e. a node does not share its own trust level with other nodes till the node knows, from the base station or any other third node, that the other node

is a good node. However, the node shares trust level of rest of the nodes. It handles multiple black nodes with short delays. The disadvantage of this approach is that a blackhole node can spread false good information. Also nodes do not share and keep any negative information. It does not handle collaborating blackhole nodes also.

In both approaches, each node in the network keeps a `Goodness table (GT) 'with two fields, Node id and trust level. Trust level takes value `good '.

4.3 Third Approach

In this approach, we introduce a node to store two more fields called timestamp and no of contacts with trust level of encountered node in its `Goodness Table(GT)'.

- Timestamp : This field represents the freshness of trust information of encountered nodes till current time stored with a node.
- No of contacts : It represents the count to keep the contact history of an encountered node for which it does not forward data packets.

Detection of bad node When a nodes say node$_A$ in contact with node$_B$, and no of contacts field of node$_A$ in node$_B$ gets greater than a threshold than node$_B$ changes trust level of node$_A$ from `good' to `bad'. This approach when combined with appraoch1, handles multiple external and internal black nodes.

5. Detection of internal blackhole node

A node initially registers its trust level to base-station or to another good node. Now, a node say node$_{IA}$ is good initially and forwards data packets to base-station or other good node say node$_B$ and register itself as good in their GT. Now with this trust level [8] of node$_{IA}$ they store a timestamp say t1. After some time, when nodeIA (after getting compromised) stops data forwarding and comes in contact with node$_B$, it does not forward any data packet to Node$_B$. Node$_B$, now starts its counter by incrementing no of contacts field. After a threshold number of contacts, node$_B$ comes to know that Node$_{IA}$ is a bad node. Node$_B$ changes trust level of node$_{IA}$ as bad and timestamp as t2. Any other node when will come in contact with node$_B$, It will check first node$_{Bs}$ goodness and then compares timestamp of its information and Node$_B$s information and stores node$_{IA}$ as bad node. This way other nodes also come to know that node$_{IA}$ is a bad node and stops forwarding data packets to node$_{IA}$.

6. Experimental Setup

We used the Opportunistic Network Environment (ONE) simulator implemented in Java to evaluate the algorithms. The ONE simulating pattern [5] of the nodes and the message exchange between them. Many of the routing algorithms are pre implemented in the simulator. We implemented the routing as used in our algorithm and the one used in
DSG by extending the functionalities available in ONE. Three metrics message delivery ratio, message traffic ratio and delay per message were used to compare the performance .The metrics message delivery ratio is used to compare the performance . The simulator generated the message delivery ratio and the message traffic but the functionality for generating delay per delivered message was added to the simulator. The experimental setup was also slightly modified to study the impact.

6.1 Data Source and Simulation Parameter

In order to objectively compare the results extensive simulations were carried out on the data obtained from an experiment conducted at University of Cambridge at the 2005 Grand Hyatt Miami IEEE Infocom conference as used in DSG. We also added the contact pattern of two periodic carrier nodes, following a fixed trajectory and a fixed time period, with other nodes in the data. For simulation purpose one of the node, as mentioned in the data, was considered to be a sink/base
station. The carrier nodes introduced in the data were neither a message producer nor a message consumer. They were designed to simply receive message from nodes and deliver it to the base station. The carrier nodes are capable of delivering the messages to base station in two hops. The simulation was run on the whole data set.

- The number of nodes in the CRAWDAD data set[1] are 9.
- Total number of messages generated were 6607.
- Message size was kept at 1MB.
- The transmission speed of nodes was 256kBps.
- The buffer space was kept at 2000MB for the DTN nodes.
- The message TTL(time to live) was set as 1 day(1440 min).
- The threshold used for group formation (Ψ) is 0.004 and for group merger(τ) is 0.300 as used in DSG.
- The probability decay rate (ϕ) is 0.075 and that of contact dacay ratio ($\dot{\alpha}$) is 0.300.

6.3 Comparison of Results

First we show the impact of presence of Blackhole on DSG in the crawdad data set. Figure 1 shows that the packet delivery drops significantly in presence of Blackhole. Figure shows that the packet delivery of DSG and decreases as the number of blackhole increases. Next, we compare the performance of DSG and our algorithms in presence of a multiple Blackhole and internal attack

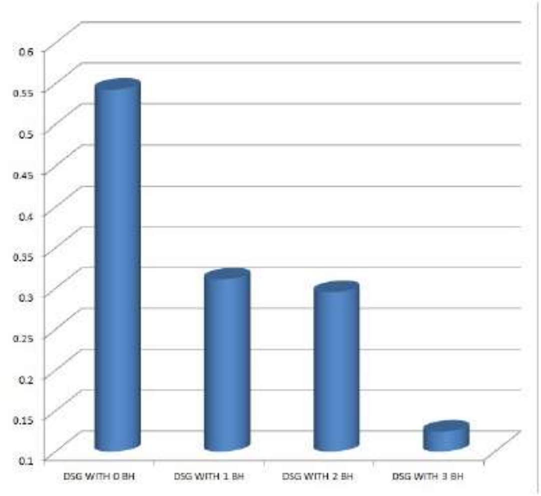

Figure 1 Delivery ratio in presence of blackhole.

Figure 2 shows the comparative results of DSG and our algorithms when 2 collaborative blackhole. nodes are present in the network .The figure shows that the packet delivery ratio improves considerably in our algorithm as compared to DSG this is due to the fact that the packets are forwarded in a delayed manner to avoid blackhole nodes.

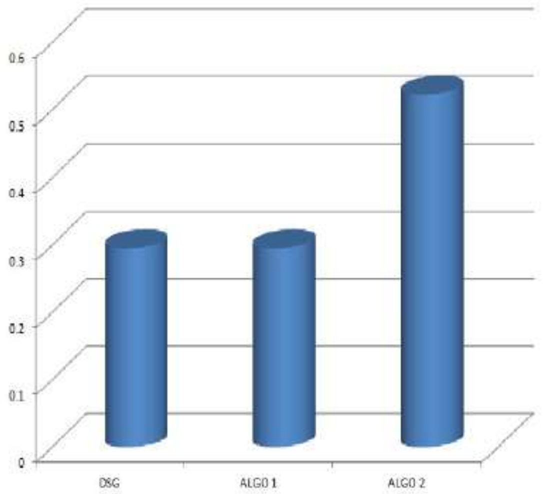

Figure 2 Comparative result of two DSG and two algorithms in presence of 2 blackhole

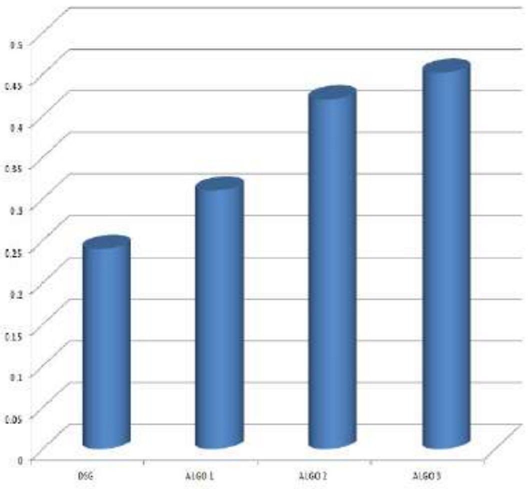

Figure 3 Comparison of message delivery ratio in presence of 2 collaborative blackhole and one internal attack

Figure 3 shows the performance of various algorithms when one or more internal nodes become malicious after some time . This figure shows the result in the presence of 2 black hole and one internal attack. As it is clear from the figure, algorithm 3 outperforms all the three algorithm in terms of the delivery probability.

7. Conclusion

We have used ONE simulator for analysing the performance of algorithms that handling the blackhole nodes. We showed impact of internal and external blackhole on social group based routing protocol (DSG) and proposed these three algorithms to mitigate the attacks with varying capability of detection. First algorithm showed better delivery of probability while did not handle collaborative blackhole. Second algorithm is robust in terms of number and collaboration among blackholes but showed little low delivery. Our third algorithm outperformed in terms of delivery and detection for internal and external blackholes in comparison with first and second. We also propose as future work on wormhole detection in social group based algorithms where in two or more malicious nodes contact each other frequently and create a tunnel among each other to attract the packets.

REFERENCES :

1. James Scott, Richard Gass, Jon Crowcroft, Pan Hui, Christophe Diot and Augustin Chaintreau. CRAWDAD data set cambridge/haggle (v. 2009-05-29). Downloaded from http://crawdad.cs .dartmouth .edu /cambridge/haggle, may, 2009.

2. V. Cerf, et al, “Delay-Tolerant Network Architecture”, IETF RFC 4838, Internet Engineering Task Force, 2007 , http://www.ietf.org/rfc/rfc4838.txt.

3. K. Fall. “A Delay-Tolerant Network Architecture for Challenged Internets”. In ACM SIGCOMM, Aug. 2003.

4. Sushant Jain, Kevin Fall and Rabin Patra. “Routing in Delay Tolerant Network”. In Proceedings of the 2004 conference on Applications , technologies, architectures and protocols for computer communications , pages 45-158 , 2004.

5. E. M. Daly and M. Haahr. “Social Network analysis for routing in Disconnected Delay-Tolerant Manets”. In Proceedings of the 8th ACM International symposium on Mobile ad hoc networking and computing , pages 32-40 ,2007.

6. A. Lindgren, A. Doria and O. Schelen. “Probabilistic Routing in Intermittently Connected Networks”. ACM SIGMOBILE Mobile Computing and Communications Review, vol. 7, 2003.

DOI: 10.18535/Ijecs/v4i12.28

7. Linton C. Freeman. “A Set of Measuring Centrality Based on Betweenness” . In Sociometry , vol. 40, pages 35-41, 1977.

8. Martin Everetta and Stephen P. Borgatti. “Ego network betweenness”. In Social Networks , Elsevier , vol 27 , pages 31-38 , 2005.

9. Pan Hui, Augustin Chaintreau, James Scott, Richard Gass, Jon Crowcroft and Christophe Diot. “Pocket Switched Networks and Human Mobility in Conference environments”. In Proceedings of the ACM SIGCOMM workshop on Delay-Tolerant networking , pages 244-251, 2005 .

10. Roy Cabaniss, Sanjay Madria, George Rush, Abbey Trotta and Srinivasan S. Vulli. “Dynamic social grouping based routing in a mobile ad-hoc network”. In Proceedings of the IEEE International Conference on Mobile Data Management , pages 295-296, 2010.

11. Roy Cabaniss , James M. Bridges , Andrew Wilson and Sanjay Madria. “DSG-N2: A Group-Based Social Routing Algorithm”. In proceedings of IEEE International Conference on Wireless Communication and Networking , pages 504-509 , 2011.

12. S. Burleigh, “Licklider Transmission Protocol – Motivation”, IETF RFC 5325, Internet Engineering Task Force, 2008 ,http://www.ietf.org/rfc/rfc5325.txt.