

A Novel technique for Blackhole GrayHole Detection under DTN: A Mathematical Model

Afroze Ansari¹ and Dr. Mohammed Abdul Waheed²

¹Research Scholar,

Dept of Computer Science & Engineering,
VISVESVARAYA TECHNOLOGICAL UNIVERSITY
Centre for PG studies, Regional office,
Kalaburagi, KARNATAKA.
anssariafroze@yahoo.com

²Associate Professor,

Dept of Computer Science & Engineering,
VISVESVARAYA TECHNOLOGICAL UNIVERSITY
Centre for PG studies, Regional office,
Kalaburagi, KARNATAKA.
dr.mawaheed@gmail.com

January 13, 2018

Abstract

DTN (Delay Tolerant network) is created to adapt to irregular connectivity and long delay in remote systems. Delay tolerance is a yet another major problems in sensor networks focusing towards a neutral drop of packets and messages are at higher concern. This improves overall performs by analysing and retrieving fundamental transporting units, that is appending a systematic procedure to black list, mark and update the malfunctioning nodes. In this paper, a systematic fault tolerance network is simulated using Statistical based detection of blackhole and grey hole

attacks and a mathematical modelling cum proof of concept is demonstrated. To recognize the misbehaviour of any individual node, this paper characterizes proportion measurements which differentiate the attackers behaviour and the ordinary ones.

Key Words : Blackhole, Greyhole, fault tolerance, SDBG, collision.

1 Introduction

SDBG has been proposed which detects both individual and collision attacks with high accuracy. We plan an identification scheme which includes two procedures: individual and collision recognition. Upon experience, the nodes in the network exchange their encounter records with one another and on the basis of that, they judge the behaviour of the other nodes. To start with, the recognition algorithm for individually attacking nodes will be executed by judging member. This node calculates sending measurements of a node which is being judged in turn thinks about those nodes in terms of predefined thresholds. On off chance that edges are disregarded, judging node diminishes trust in past judgment on one. Something else, conspiracy discovery procedure carried by the judging node includes doubt and confirmation as the different stages of procedure.

Improved IF plans ready to secure against sophisticated collusion attacks by giving an initial estimate of reliability of sensors utilizing inputs and outputs. We give an exhaustive experimental evaluation of efficiency and effectiveness of our proposed aggregation technique. The outcomes demonstrate that our technique gives both higher accuracy and preferable collusion resistance over the existing strategies. To the best of our insight, none of the existing system addresses on false information injection for various straightforward attack situations, on account of a collusion attack by malicious nodes in a way which utilizes high level learning about information collection algorithm used.

2 Literature survey

- According to [1], the exceedingly effective design and protocols of the present Internet may work ineffectively in situations described by long delay ways and regular system segments. The design works as an overlay over the vehicle layers of the systems it interconnects, and gives enter administrations.
- According to [6] over the previous decade, mobile computing and remote communication have turned out to be progressively critical drivers of numerous new computing applications. The field of remote sensor organizes especially concentrates on applications including self-ruling utilization of process, detecting, and remote specialized gadgets for both logical and business purposes. This paper looks at the examination choices and plan trade-offs that emerge while applying remote shared systems administration methods in a portable sensor arrange intended to help natural life following for science explore.
- According to authors of [10], the DTNs are helpless against insider attacks, in which the genuine nodes are compromised and the attackers alters the delivery measurements of the nodes to dispatch harmful attacks in the systems. We assessed our approach through broad simulations utilizing both Random Way Point and Zebranet versatility models. Our outcomes demonstrate that MUTON can identify insider assaults effectively with identification rate and low false positive rate.
- According [15], in DTNs, malicious and selfish nodes may drop the received packets. Circulated plan has been introduced for distinguishing the dropping of data packets. This paper includes a plan, in which a node has to store the noticeable previous contact records, in the view of following reached nodes, which recognizes the packets dropped in the network. We likewise suggest a plan for mitigating misbehaviour with the help of constraining packets quality sent to falsely behaving ones.

- In [18], experimental results have shown that the behaviour of genuine connections in low-power remote systems, (for example, remote sensor systems) strays to some vast degree from the ideal binary model utilized in many number of simulation studies. We give a comprehensive analysis of main causes of asymmetry and unreliability.

3 System design

Fig 1.1 After creating the network topology, trust authority mentions a particular node to be a suspicious node. Data will be sent through the intermediate nodes. The routing addresses will be sent to the trust authority. Received encounter addresses will be compared. If the encounter records are equal then the data will be transmitted successfully otherwise that node will be marked as a malicious node.

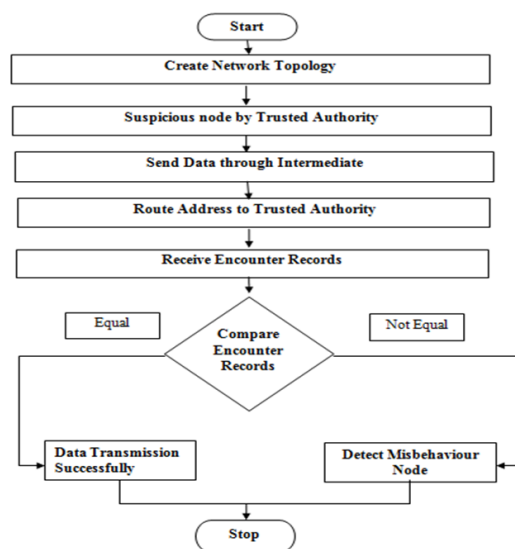


Fig 1.1 System design of SDBG

4 Mathematical modelling

4.1 Network establishment

Normal nodes : $\{n_1, n_2, n_3, \dots, n_n\}$

Where n is the maximum number of normal nodes

Network also consists of malicious nodes (m)

Where m can be a greyhole or blackhole node

Let us consider N is a network

Such that $N = \text{Sum}(m, n)$

That is $m \in N \ \&\& \ n \in N$ / Case 1: $n \not\in m \ \forall$ if n is originated of N

Case 2: $m \in n \ \forall$ if m is a tampered node

4.2 Transmission activation

Establishment and observation of Encounter records (ER) where ER consist of ratio confidential of transmission

$$(E_R)_I > \{(E_R)_{i-1}\}_N]_n + \{(E_R)_{j-1}\}_N]_m$$

Where j =fake ratio of E_R in m and trapped with $n/(m, n \in N)$

4.3 Scenario generation

Formation of attackers that is A is a node under N and is originated in m / $A \in m$

Where $A = A_1, A_2, A_3, \dots, A_j$

Where j is the maximum ratio of m

that is $j < m \ \&\& \ A \in j$ but $j \notin A$.

Faking encounter records:

$$\text{Assume } (E_R)_{matrix} = \{(E_R)_1, (E_R)_2, \dots, (E_R)_n\} + \{(E_R)_m\}$$

$$(E_R)_{matrix} = \{(E_R)_1 + (E_R)_2, \dots, (E_R)_n + (E_R)_j\}$$

$\forall \{(E_R)_i\}_{matrix} = \sum_{i=0}^N [(E_R)_{i+1} < (E_R)_i]$ / Extract forwarding ratio for transmission

4.4 Judgement node creation and validation

If $(E_R)_i$ is computational aggregate for $(E_R)_{i-1}$ in N then regard (E_R) as judging node Validating of judged node under isolated attack

Threshold analysis $(T_d) = \{T_1, T_2, \dots, T_n\} / (E_R)_i \in T_d$

And $T_d \geq (E_R)_I \& T_d \in (N)_T$

Where $N_T = \{N_{T1}, N_{T2}, N_{T3}, \dots, N_{Ti}\}$

Computing $(T_d)_{(ER)_i}$ that is 5 is the representation of $(T_d)_{(ER)_i}$

$5 = J\{(N_T)_i < (E_R)_i\}$

Case 1: if $J(E_{Ri})++$ that is confidence enhancement of judged node

Else

Case 2: $J(E_{Ri}) - \& \& F(i)]_m$

Where $F(i)]_m$ is a flagging operation to identify as malicious node but not confirmed

4.5 Validation and verification under performance evaluation

On validation $F = \{F_1, F_2, F_3, \dots, F_g\}$

$F = \sum[(F_i)_{conf}]_0^N + \sum(m_j)++$

Monitor (m_j) under successive transmission on record (performance) Then repeat step 4 and 5 for confidence revaluation and elimination

5 Evaluation

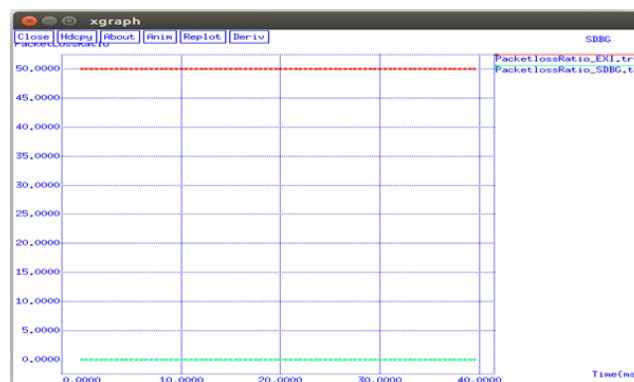


Fig 1.2 Packet loss ratio

The packet loss of proposed system is zero whereas the packet loss ratio of the existing system is much higher

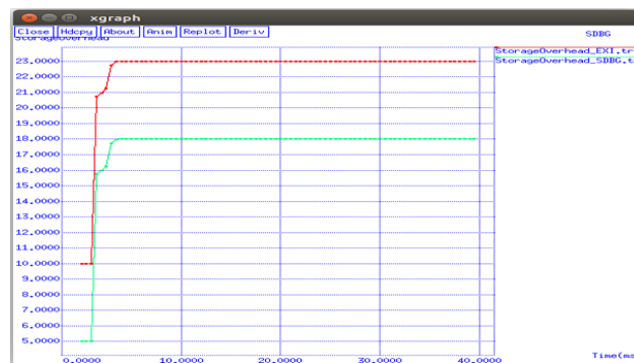


Fig 1.3 Storage overhead

The storage overhead in the proposed system is lesser when compared with the storage overhead of the existing system

6 Conclusion

Among the various risks to the wireless systems and delay tolerant networks, blackhole and greyhole attacks are the most prominent. Most of the previous works were on defending against the issues of packet dropping in the delay tolerant networks, but among which most of them failed to prevent the collusion attacks done by the malicious nodes present in the network. This technique is centric towards SDBG attacks that can effectively prevent not only the individual attackers as well as coordinating attackers.

The simulation results say that packet delivery ratio achieved by the proposed system is greater than the packet delivery ratio of the existing system, packet loss ratio of proposed system is zero whereas the packet loss ratio of the existing system is much higher, end to end delay seen in the proposed system is much lower than the end to end delay of the existing system and also storage overhead in the proposed system is lesser when compared with the storage overhead seen in the existing system. The future work will be to check the reliability of a node in the network which is surrounded by malicious

nodes and to encounter records of a node by its neighbours if one particular node is a new node to defined network.

References

- [1] K. Fall, *A delay-tolerant network architecture for challenged internets*, in Proc. Conf. Appl., Technol., Archit. Protocols Comput. Commun., 2003, pp. 2734.
- [2] M. J. Khabbaz, C. M. Assi, and W. F. Fawaz, *Disruption-tolerant networking: A comprehensive survey on recent developments and persisting challenges*, in Proc. IEEE Commun. Surveys Tuts., 2012, vol. 14, pp. 607640.
- [3] *Delay-tolerant networking research group* [Online]. Available: <http://www.dtnrg.org/wiki>
- [4] S. Burleigh, V. Cerf, R. Durst, K. Fall, A. Hooke, K. Scott, and H. Weiss, *The interplanetary internet: A communication infrastructure for Mars exploration*, in Proc. Committee Space Res. Sci. Assem., 2002, 36537.
- [5] J. Partan, J. Kurose, and B. N. Levine, *A survey of practical issues in underwater networks*, in Proc. 1st ACM Int. workshop Underwa-terNetw., Sep. 2006, pp. 1724.
- [6] P. Juang, H. Oki, Y. Wang, M. Martonosi, L. S. Peh, and D. Rubenstein, *Energy-efficient computing for wildlife tracking: Design tradeoffs and early experiences with ZebraNet*, in Proc. 10th Int. Conf. Archit. Support Program. Lang. Oper. Syst., Dec. 2002, pp. 96107.
- [7] S. Guo, M. H. Falaki, E. A. Oliver, S. Ur Rahman, A. Seth, M. A. Zaharia, and S. Keshav, *Very low-cost Internet access using KioskNet*, in Proc. ACM SIGCOMM Comput. Commun. Rev., Oct. 2007, vol. 37, no. 5, pp. 95100.
- [8] J. Ott and D. Kutscher, *A disconnection-tolerant transport for drive-thru internet environments*, in Proc. IEEE 24th Annu. Joint Conf. Comput. Commun. Soc., Mar. 2005, pp. 18491862.

- [9] M. Chuah, P. Yang, and J. Han, *A ferry-based intrusion detection scheme for sparsely connected ad hoc networks*, in Proc. 4th Annu. Int. Conf. Workshop Security Emerging Ubiquitous Comput., 2007, pp. 18.
- [10] Y. Ren, M. Chuah, J. Yang, and Y. Chen, *MUTON: Detecting malicious nodes in disrupt-tolerant networks*, in Proc. IEEE Wire-less Commun. Netw. Conf., 2010, pp. 16.
- [11] Z. Gao, H. Zhu, S. Du, C. Xiao, and R. Lu, *PMDS: A probabilistic misbehavior detection scheme toward efficient trust establishment in Delay-tolerant networks*, IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 1, pp. 2232, Jan. 2014.
- [12] N. Li and S. K. Das, *A trust-based framework for data forwarding in opportunistic networks*, Elsevier J. Ad Hoc Netw., vol. 14, pp. 14971509, 2013.
- [13] F. Li, J. Wu, and A. Srinivasan, *Thwarting blackhole attacks in disrupt-tolerant networks using encounter tickets*, in Proc. INFOCOMM, 2009, pp. 24282436.
- [14] Y. Guo, S. Schildt, and L. Wolf, *Detecting blackhole and grey-hole attacks in vehicular delay tolerant networks*, in Proc. IEEE 5th Int. Conf. Commun. Syst. Netw., Jan. 2013, pp. 17.
- [15] Q. Li and G. Cao, *Mitigating routing misbehaviors in disruption tolerant networks*, IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 664675, Apr. 2012.
- [16] A. Keranen, J. Ott, and T. Karkkainen, *The one simulator for dtn protocol evaluation*, in Proc. 2nd Int. Conf. Simul. Tools Tech., Rome, Italy, Mar. 2009, pp. 55:155:10.
- [17] A. Lindgren, A. Doria, and O. Schelen, *Probabilistic routing in intermittently connected networks*, SIGMOBILE Mobile Comput. Commun. Rev., vol. 7, pp. 1920, 2003.
- [18] R. Patra, S. Surana, and S. Nedeveschi, *Hierarchical identity based cryptography for end-to-end security in DTNs*, in Proc. Intell. Comput. Commun. Process., 2008, pp. 223230.

