Engineering Universe for Scientific Research and Management
(International Journal)
ISSN(ONLINE) : 2319-3069
Vol. 8 Issue 9
September 2016

Review on Secret Sharing Towards Enhancing the Reliability of Mobile Ad Hoc Network

Nisha Bharti[1], Hansa Acharya[2]
Department of Computer Science & Engineering
Radharaman Institute of Technology and Science, Bhopal[1, 2]
nnishabharti@gmail.com[1], hansaacharya@gmail.com[2]

Abstract
Mobile Adhoc Networks (MANET) has become the most important means of communication in our day to day life. A rapid advance in technology and proliferation of wireless devices in the recent times has attracted huge attention towards research on MANET. It has found wide applications in dynamic and infrastructure less environments including emergency rescue operations etc. However, very little work is reported in the literature regarding reliability analyses for MANET. The paper presents survey of reliability analysis for MANET and provides critical reviews on them. Challenges in reliability analyses of MANET are also highlighted in the paper.

Keywords: Network reliability; Mobile adhoc network; Routing Protocols, Secret sharing, cheater participant, Data exchange.

1. Introduction

A Mobile Ad-Hoc network (MANET) is an infrastructure- less network of wireless mobile devices connected by wireless links that forms a temporary network. Every mobile device/node in MANET [1][2] is free to move randomly. Hence the topology of MANET also changes dynamically. Every mobile node can communicate with each other when found within the communication range of each other. MANET is also called multi-hop wireless network. MANETs have become one of the inevitable parts in our daily communication systems. It has also become very suitable means of communication during emergency cases such as rescue operations where there is a need to build temporary wireless application without infrastructure. There has been considerable demand for reliable communication due to the technological innovations in recent times. Hence, reliability of MANET has become an important area of research today.

An increasing dependence on more reliable services implies that there is a need to incorporate reliability analysis as an integral part in their planning, design and operation of systems. A system is highly reliable i.e. mostly available, if there is a negligible probability that the system will be down at any instant of time of usage. MANET reliability is an important benchmark for reliable communication. The qualitative definition of network reliability is the ability of the network to continue services in the case of component failures [3]. The quantitative definition of network reliability is the probability of existence of at least one path between a specified numbers of k-nodes under known conditions [4]. Therefore, network reliability of MANET must focus on communication. The progression communication of MANET is fragile compared to wire network due to some of its attributes such as dynamic topology, environment without infrastructure, multi-hop routing, node mobility, rapid deployment, constrained resource, flexibility, self-organizing, specific application, MANET types i.e. homogenous or heterogeneous etc. Most of these attributes affect the continuity of network connectivity and hence they are important for measuring the network reliability of MANET. Reliability analysis may refer to two-terminal, k-terminal and all-terminal reliabilities of a traditional network where each node is considered as a terminal. The successful communication between a pair of nodes is defined as the presence of one or more operating paths between the nodes. The probability of successful communication between two nodes of the network is called two-terminal reliability [4][6]. It is the probability of successful transmission of a message from source node to destination node. The probability of

Engineering Universe for Scientific Research and Management
(International Journal)
A Universe of Research
ISSN(ONLINE) : 2319-3069
Vol. 8 Issue 9
September 2016

successful communication between a node and all other nodes of the network is called all-terminal reliability i.e. the probability that node ni can communicate with node nj for all pairs ninj where i≠j. The k-terminal reliability is the probability that a subset of k nodes are connected where 2≤ k ≤ n. The metric that will give the probability that the operating nodes can successfully communicate is the all-operating terminal reliability [7]. This is useful for reliability analysis of nodes that are disconnected due to lack of communication links rather than disconnection as a result of radio failure.

Most reliability analysis is focused on all-terminal reliability. This is true for MANET because based on this analysis, protocol design and complex MANET deployment can be guided. The methods used for traditional infrastructure based networked systems i.e. enumeration, transformation, reduction, decomposition, factoring theorem etc. cannot be used directly for analysis/computing the reliability of MANET. This is because we must consider node reliability, link reliability and node mobility model (that gives rise to dynamic topology having many configurations) for computing all terminal reliability of MANET [7][8]. Additionally, network congestion is more serious in MANET compared to that of traditional networks because of multi-hop channel routing and node mobility. This will lead to dropping of packets and will affect all terminal reliability of MANET.

The remainder of the paper is put in order as below. Section II presents survey of reliability analysis for MANET along with brief description of the work done in each paper. Section III provides some challenges of reliability analysis of MANET. Conclusions are drawn in section IV and References are given at the end.

2. Secret Sharing

Secret sharing is the workmanship and exploration of implanting data into a spread article without the presence of the concealed messages. Inexorably, concealing some information will change the cover text regardless of the fact that the distortion created by secret text stowing away is vague to the human visual framework. Then again, for a few applications, for example, restorative picture framework, law requirement, military symbolism and fine art conservation, it is alluring to switch the stego - text once more to the first cover picture without any distortion after information extraction. A few strategies have been distributed that fulfill this reversibility prerequisite.

The basic idea of secret sharing is to divide information into several pieces such that certain subsets of these pieces (shares) can be used to recover the information. Where face player want to retrieve several shared information. In order to make participate in reconstruction of secret information and try to destroy the information.

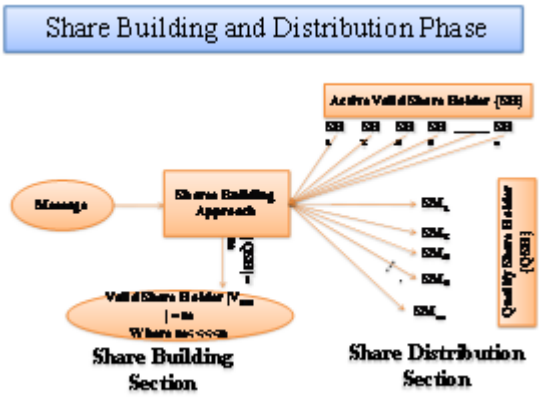

Figure 1 Secret Building & Distribution Section

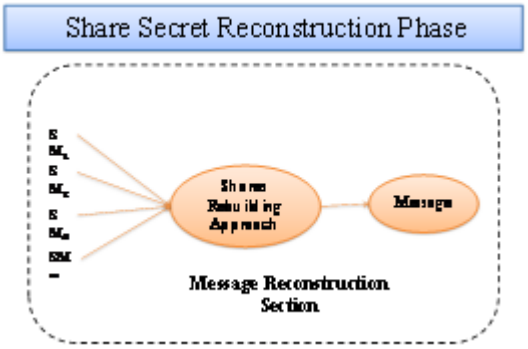

Figure 2 Secret Reconstruction Phase

Secret sharing scheme having three different phases namely share building phase, share distribution phase and secret reconstruction phase Steganography is one of the methods used for the hidden exchange of information and it can be defined as the study of invisible communication that usually deals with the way of hiding the existence of the communicated message. In this way, if successfully it is achieved the message does

not attract attention from eaves droppers and attackers. Using Steganography Information can be hidden in different embedding mediums, known as carriers. These carriers can be images, audio files, video files, and text files.

3. Related Work

A Mobile Ad-hoc Network (MANET) has been studied in order to realize a ubiquitous society. However, MANET has many issues. One of the issues is security. This section evaluates different research that has been carried out in MANET security field till now. Kei Kobayashi present secure communication method using secret sharing scheme over MANET by adding dummy packet transmission and storing multiple shares in a single packet. And also the improvement achieves packet reduction that results in energy saving and collision reduction. But still needed to realize more improvement in reach ability of secure communication and to clarify how to decrease the number of non-member nodes that are capable of restoring a secret information [9]. AboElFotoh have addressed two-terminal reliability computation for radio-broadcast networks with the condition of failure of nodes only. However, they have not provided any relation between link failure probability and relative motion of the nodes [10]. Kumar presented a method to optimize network reliability, network diameter and distance using genetic algorithm [11]. Dengiz proposed a heuristic approach for communication networks towards solving topological reliability allocation problems. The aim was to apply the heuristic approach for reducing the NP-hard problem for networks having large search spaces [12]. Turgut and Chatterjee provided the review of the effect of mobility models on the life span of communication path existence in MANET [13]. Levitin has presented an algorithm to determine the optimal distribution of elements within the network infrastructure to provide the highest terminal reliability. This algorithm is used for allocation of multi-state elements in communication networks [14]. Adickes have used genetic optimizer to optimize the geographic layout of nodes in indoor wireless networks that may be used to extend local area networks [15]. H. Bhatt have described the effect of mobility on the bit error rate (BER) and minimum node spatial density of an ad-hoc network for obtaining full connectivity. They used BER as the network performance metric. However, the chances of node failure while accounting for total network connectivity were not considered [16]. Ye proposed a node deployment strategy to increase the probability of a reliable path. This was achieved by placing nodes at strategic locations and possibility of practically controlling node mobility and limiting its use to such instances [17]. J. Chung has provided review of the situation where the nodes have an exponentially distributed finite lifetime between source and destination [18]. K. Rocco and Muselli have provided comparisons of various machine learning techniques to develop approximate reliability expressions for capacitated networks [19]. L. Ramirez-Marquez and Coit have proposed methods to address both multi-state and capacitated network reliability. They provide multiple methods of addressing the reliability allocation optimization problems in the presence of common cause failures [20]. M. Marseguerra have proposed an approach to incorporate uncertainty into reliability calculations by using Monte Carlo simulation and genetic algorithm [21]. N. Chen and Lyu have described the process of mobile cell phone transition from one tower to another. They used Markov model to represent the network configuration change as one cell phone moves from one coverage area of one tower to the other area covered by another tower. They expressed network reliability as a function of the reliability of each node active in that configuration and the percentage of time that each configuration exists. This is not applicable to MANET since mobility of the nodes is not modeled. They assumed that failure of any active node in the path of a message results in failure which shows that configuration is a series system. This assumption is not suitable for MANET as extra paths may be found in between source and destination nodes [22]. O. S. Kharbash and W. Wang have derived a symbolic two-terminal reliability expression for MANET that can handle imperfect nodes in the dynamic network connectivity. They have focused on reliability of node and link for static topologies and presented the effect of the rate of node failure and mobility pattern on the two-terminal reliability of MANET [23]. P. Brooks have analyzed mobile sensor multi-hop networks using a combination of percolation theory, random graph theory and linear algebra. They used a probabilistic adjacency matrix to analyze the network connectivity. However,

they have not addressed the mobility of mobile nodes [24]. Cook, Jason L have provided the analytical concepts of Adhoc networks along with Monte Carlo simulation to determine the two-terminal reliability of MANET. They considered the existence of a communication link as a probabilistic event with respect to the status of network nodes [25]. R. Cook, Jason L have provided the method using Monte Carlo simulation to determine the two-terminal reliability of MANET by addressing mobility of nodes, considering the existence of a communication link as a probabilistic event with respect to the status of network nodes. The reliability estimate comes out to be conservative which may not be practical for large MANET [26]. S. Fei Huang have shown the theoretical use of logistic regression method to compute the reliability of wireless sensor networks and other parameters [27]. T. S. K. Chaturvedi and N. Padmavathy have illustrated the effects of network size, transmission range and network coverage area on the reliability measures by modeling MANET as geometric random graph. They applied a Monte Carlo simulation to evaluate reliability of MANET whose node failure is governed by a known statistical distribution where links between the nodes are established dynamically depending on the transmission range of nodes. They emphasized on the influence of scenario metrics on the MANET reliability [28]. Xibin Zhao have presented a novel two-terminal reliability analysis for MANET by proposing an effective Monte Carlo method [29] . They analyzed node mobility effect and node reliability on a real MANET platform. V. Singh, M.M., Baruah, M. and Mandal J. K have proposed a method to compute the reliability of MANET using logistic regression and they provided simulation results to support the correctness of their method [30].

4. Challenges in MANET Reliability Analysis

Very little research work has been done for the reliability analyses of MANET till now which is evident from the literature. MANET has been considered as the most useful means of communication due to its important features such as infrastructure less environment, mobility etc. However reliability of MANET is weak compared to traditional networks. MANET has several aspects that make them vulnerable to failures and connectivity problems. The MANET devices have limited power, transmission range and ability to change locations. Hence, reliability analyses of MANET have become inevitable now. Network reliability computation methods are useful tool for network design, implementation and performance evaluation. Network reliability research is concerned with the development of techniques and methods for its computation and network reliability optimization is a field of research into itself [27].

The aim of MANET reliability analysis is to quantifying the network services and identifying the weakness in the network due to component failures [29]. The probabilistic consideration of existence of a link and specific mobility profile of a node in MANET is a challenge Computation of MANET reliability under specific node mobility and existence configurations need attention as node failures are transient in nature.

5. Conclusion

Ensuring the reliability of MANET has attracted huge attention in the recent times due to emergence of mobile wireless communication system. Ability to analyze reliability is foundation for ensuring the reliability of MANET. Reliability analysis can be a quantitative analysis using mathematical modeling. Reliability computation methods are important tool for reliability analysis.

The paper has reviewed and presented reliability analysis for secret sharing in mobile ad-hoc network (MANET). It has focused on some key issues and challenges in MANET reliability analysis. Since very little research work is available in the literature as of now, more research on MANET reliability computation and analysis is required.

Reference

[1] Toh, C. K. “Adhoc Mobile Wireless Networks: Protocols and Systems”, Prentice Hall Publications 2002.
[2] Sarkar S. K., T. G. Basavaraju and C. Puttamadappa, “AdHoc Mobile Wireless Networks: Principles, Protocols and Applications”, Auerbach Publications, 2008.
[3] R. Billinton and R. N. Allan, “Reliability Evaluation of Engineering Systems: Conncepts and

Techniques", Springer International Edition, 2nd Edition, Indian Reprint 2007.
[4] Charles J. Colbourn, "The Combinatorics of Network Reliability", Oxford University Press, New York, 1987.
[5] Martin .L. Shooman, "Probabilistic Reliability: An Engineering Approach", 2nd Edition Melbourne, FL,1990.
[6] M. L. Shooman, "Reliability of Computer Systems and Networks", J. Willey, NewYork, 2002
[7] Cook JL, Ramirez-Marquez JE. "Optimal design of cluster-based ad- hoc networks using probabilistic solution discovery", Reliability Engineering and System Safety 94(2009) 218-228.
[8] Laxmi Shrivastava, G. S. Tomar & SS. Bhadauriya, "A Survey on Congestion Adaptive Routing Protocols for Mobile Ad-Hoc Networks", International Journal of Computer Theory and Engineering, Vol.3 No.2, pp 189-196, Apr 2011.
[9] K. Kobayashi, Y. Totani, K. Utsu and H. Ishii, "Improvement of Secure Communication Method Using Secret Sharing Schemes over MANET," Information Science and Security (ICISS), 2015 2nd International Conference on, Seoul, 2015, pp. 1-4.
[10] AboEIFotoh HM, Colbourn CJ. Computing 2-terminal reliability forradio-broadcast networks. IEEE Trans Reliab 1989;38(5):538–55.163
[11] Kumar A, Pathak R, Gupta Y, "Genetic algorithm based reliability optimization for computer network expansion", IEEE transaction on reliability 1995;44(1):63-72.
[12] Dengiz B, Altiparmak F. Smith AE., "Efficient optimization of all- terminal reliable networks using an evolutionary approach", IEEE transactions on Reliability 1997;46(1):18-26
[13] Turgut D, Das SK, Chatterjee M. Longevity of routes in mobile ad hoc networks. In: Proceedings of IEEE vehicular technology conference (VTC), vol. 4, Spring; 2001. p. 2833–7.
[14] Levitin G., "Optimal allocation of multi-state retransmitters in acyclic transmission networks", Reliability Engineering and system safety 2002;75:73-82.
[15] Adickes M, Billo, R., Norman B, Banerjee S, Nnahi B, Rajagopal J, "Optimization of indoor wireless communication network layouts", IIE transaction 2002; 34:823-36.
[16] Bhatt M, Chokshi R, Desai S, Panichpapiboon S, Wisitpongphan N, et al. Impact Of mobility on the performance of ad hoc wireless networks. IEEE 58th vehicular technology conference, vol. 5, 6–9 Oct, 2003. p. 3025–9.
[17] Ye Z, Krishnamurthy S V, Tripathi S K, "A routing framework for providing robustness to node failures in mobile adhoc networks", Adhoc Networks 2004;2(1):87-107
[18] Chung W-H. Probabilistic analysis of routes on mobile ad hoc networks. IEEE Commun Lett 2004; 8(8).
[19] Rocco CM, Muselli M. Empirical models based on machine learning techniques for determining approximate reliability expressions. Reliab Eng Syst Saf 2004; 83(3):301–9.
[20] Ramirez-Marquez JE, Coit DA. Heuristic for solving the redundancy allocation problem for multistate series-parallel systems. Reliab Eng Syst Saf 2004; 83(3): 341–349.
[21] Marseguerra M, Zio E, Podofillini L, Coit DW. Optimal design of reliable network systems in presence of uncertainty. IEEE Trans Reliab 2005; 54(2).
[22] Chen Z, Lyu MR. Reliability analysis for various communication schemes in wireless CORBA. IEEE Trans Reliab 2005; 54(2): 232– 42.
[23] S. Kharbash and W. Wang, "Computing two-terminal reliability in mobile adhoc networks", proceedings of IEEE wireless communications and networking conference(WCNC '07), PP.2833-2838, March 2007.
[24] Laxmi Shrivastava, G.S. Tomar & Sarita Bhadoria, "Secure and Congestion Adaptive Mechanism with Load Balancing for MANETs", International Journal of Communication Systems and Networks, Vol.1 No.1, pp41-51, Feb 2012.
[25] Brooks, R. R, B. Pillai, S. Racunas and Suresh Rai , "Mobile Network Analysis Using Probabilistic Connectivity Matrices", IEEE transactions on System, Man and Cybernetics- Part C: Applications and Review, 2007; 37(4);694-702
[26] Cook JL, Ramirez-Marquez JE, "Two-terminal reliability analyses for mobile adhoc wireless network", Reliability Engineering and System Safety, 2007; 92(6); 821-829.
[27] Cook JL, Ramirez-Marquez JE. "Mobility and Reliability Modeling for a mobile ad-hoc networks", IIE Transactions, 2009; 41(1);23-31.
[28] Fei Huang, Zhipeng Jiang, Sangua Zhang, Suixiang Gao, Communication and Mobile Computing, DOI:10.1109/CMC.2010.49
[29] Chaturbvedi , S.K. , Padmavathy N. "The Influence of Scenario Metrics on Network Reliability of Mobile Adhoc Network" International Journal of Performability Engineering Vol 9, No. 1 , January 2013. pp .61 -74.

[30] Xibin Zhao, Zhiyang You and Hai Wan, "A Novel two-terminal reliability analysis for MANET", Journal of Applied Mathematics, volume 2013,article ID 216186
[31] Laxmi Shrivastava, SS. Bhadauria, G.S. Tomar, "Influence of Traffic Load on the performance of AODV, DSR and DSDV in MANET", International Journal of Communication Systems and Network Technologies, Vol.1 Issue 1. pp 22-34, Apr 2013.
[32] Singh, M.M., Baruah, M, Mandal, J.K, "Reliability Computation of Mobile Adhoc Network Using Logistic Regression", IEEE Xplore, DOI: 10.1109/WOCN.2014.6923060,2014. 164.