International Journal of Engineering & Technology, 7 (2.8) (2018) 149-155

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

Probabilistic security analysis through path-based metric evaluation in wireless sensor networks

Sampath Kumar Pattem [1] *, Jayasankar K [2], Sumalatha V [3]

[1] *Assistant Professor, Department of ECE, Malla Reddy Institute of Technology, Hyderabad, AP, India*
[2] *Professor & Head, Department of ECE, Vasavi College of Engineering, Hyderabad, AP, India*
[3] *Associate Professor, Department of ECE, JNTU college of Engineering, Anantapur, AP, India*
**Corresponding author E-mail:*

Abstract

This paper analyzes the possible security threats in the wireless sensor network (WSN) through the path based metrics. Since the routing in WSN focuses towards the energy optimizing by which an optimal path is selected which consumes less energy. However security is also very important in WSN which won't considers in the optimal path selection. This paper analyzes the possible security threats based on the characteristics of paths. A simple comparative analysis is carried out in this paper between different topologies of network through the path based metrics. Since there exists number of path metrics, some metrics are categorized as decisive and some are assistive and based on the obtained count, one network topology is finalized as more secure. Matlab is used for the Realization of this methodology.

Keywords: *WSN; Security Metrics; Shortest Path; Number of Paths; Mean Path Length; Matlab.*

1. Introduction

With the rapid development and advancement of wireless sensor technology, wireless sensor networks (WSNs) are widespread in a variety of areas, including environmental monitoring, battle field observation, intelligent home systems, forest fire detection, and health monitoring [1]. Due to the self-organizing, dynamic and data-centric characteristics of WSNs, they are deployed in more and more data observation fields, and the nodes in WSNs should cooperate with each other for communication and support of high-level applications. However, security issues have accompanied the wide use of WSNs. Because of the openness of the deployed environment and the transmission medium, WSNs suffer from various attacks, including hijack attacks, tampering attacks, DoS attacks, selective forwarding attacks, and sinkhole attacks [2].

The security evaluation in WSN can be accomplished in different aspects. Since there exists some attacks that can be occurred through the paths, there is a need to evaluate all the possibilities that an attacker can try to compromise the network by knowing the path attributes. A Path is a route that is established between a distinct source and destination node pair. In the WSN, the source follows multihop routing mechanism to transfer the data to destination node. Hence there is possibility of number of paths which differs from each other with respect to the intermediate nodes involving in the transmission. Based on these aspects, some metrics are derived to analyze the possible threats over the WSN, particularly through the knowledge about available paths and their characteristics like the path length. According to the Nwokedi Idika and Bharat Bhargava [3], the basic path based metrics are three. They are Shortest Path (SP) metric, Number of
Paths (NP) metric and Mean Path Length (MPL). Further they proposed four new metrics based on the MPL as an extended metrics for these three basic metrics and which helps to analyze the all possible security threats, effectively.

In this paper a new security metric is evaluated to analyze the security issues in WSN. This paper proposed a Number of Shortest Path (NSP) metric to measure the number of shortest paths available from the total available paths or form Number of Paths metric. The shortest path metric gives the information about the least amount of effort than an attacker can put for violating security policy. But, in an WSN, the shortest path can be measured in two ways. One is based on number of hops and another is based on distance. The proposed new metric evaluates the shortest path metric by considering both issues. This paper also proposed an extended metrics for security evaluation to overcome the above mentioned problems. Based on the all the metrics evaluated, two different network topologies are compared to find which is more secure. Including the proposed new metrics, totally the number of metrics is eight. Among these some metrics are categorized as decisive and remaining are as assistive and based on the final count for both topologies, one topology is finalized as more secure.

Rest of the paper is organized as follows: section II gives the details of the earlier metrics and their drawbacks. Section III gives the details about the proposed metric. Section IV illustrates the details about the results obtained through realization of proposed approach. Section V concludes the paper.

2. Related work

The security metrics were broadly classified into two categories as,

1) Non-path analysis based security metrics and
2) Path analysis based security metrics.

Copyright © 2018 Sampath Kumar Pattem et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

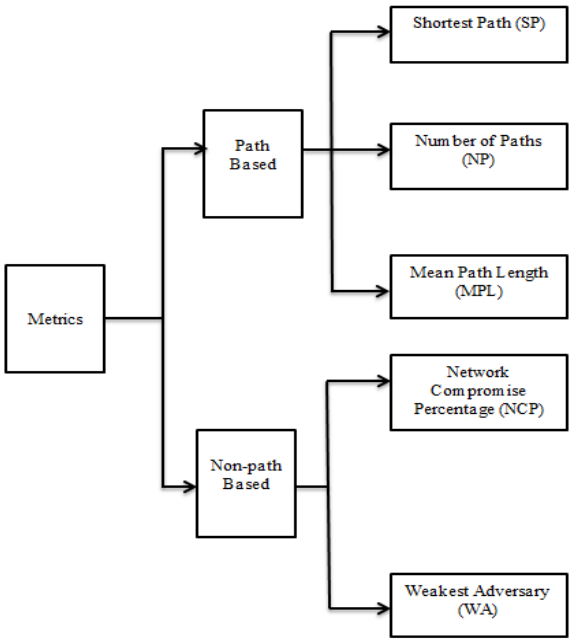


Fig. 1: Classification of Security Metrics.

2.1. Non-path analysis security metrics

1) The Network Compromise Percentage Metric (NCP) [4].
2) The Weakest Adversary Metric [5].

2.1.1. The network compromise percentage metric (NCP)

NCP metric indicates the percentage of network assets an attacker can compromise. The NCP is number of machines that are compromised by attacker on the host to obtain the access at administrator or user level. The number of compromised machines are high, the higher the value of NCP. However the main drawback is the NCP is not goal oriented. In this type of networks, the attacker has no target and it tries to compromise as possible as more number of machines. The main intention of attacker is to attain the assets of the possible machines as much as possible. This increases computational complexity and also increases analysis time consumption. For a large network with huge node count, this metric is not suitable for analysis.

2.1.2. The weakest adversary metric (WA)

The Weakest Adversary metric attempts to express the security of the network in terms of the weakest part of the network. The intuition of the metric is that one's network is no stronger than the weakest adversary, that is, the adversary with the weakest set of capabilities. Weakness of an adversary is correlated with the initial attributes of the network. Each network has some set of initial attributes that allows for the realization of a security policy violation. If comparing the security of two networks, the network requiring a weaker set of initial attributes to compromise the network is deemed less secure. The main drawback of WA, this metric assumes that there are initial conditions or attributes, but the assumption of initial attributes leads to complexity.

2.2. Path analysis security metrics

The security metric those are defined with respect to the path of the network are called path based security metrics. Since the attacker can achieve the access over the network through the paths, the understanding of paths is critical for network security analysis. Here the quantitative approach is processed for security analysis through path based metrics. It is different form the metrics those are based on graph that requires the utilization of probabilities of successful attacks [6], [7], [8]. The list of path based metrics is;

1) Shortest path metric (SP) [9].
2) Number of paths metric (NP) [10]
3) Mean of Path lengths Metric (MOPL) [11]

2.2.1. Shortest path metric (SP)

The SP [9] describes the details of an attack path which have smallest length. In this metric, the distance between the attacker's starting state to the required goal state is very short (i.e., where the violation of security occurs). The length of an attack path may be the number of conditions (nodes), the number of exploits (links), or the number of conditions and exploits that start from the attacker's initial state and proceeds in series to the attacker's goal state. The intuition underlying the Shortest Path metric is that from the perspective of the attacker, given the option of different steps the attacker can take to violate a security policy, the attacker will choose the series of steps that require the least amount of effort. Let $p_1, p_2, \ldots, p_N$ be the number of paths, the shortest path can be derived as the path which is having minimum number of hops. Since this metrics only gives information about the shortest distance but not about the number of such paths, the security analyzed can't predict the ways that an attacker trying to compromise the network through shortest paths. This metric is not adaptable to utilize in the security evaluations for real time networks independently.

2.2.2. Number of paths metric (NP)

The NP metric [10] denotes a value that describes the details of the possible number of ways to compromise the network be leveraging the network dependencies through vulnerabilities [12] to violate the security policy. The numbers of attack paths that are existing between the node sin the network are represented by this metric. Let $p_1, p_2, \ldots, p_N$ be the number of paths, the NP metric is evaluated by simply counting the total number of paths. The main objective behind this metrics to find the total possible ways that an attacker can violate the security policy without being detected at any instant. In a comparison between two topologies with different NPs, the topology with high NP value is observed to be less secure. More attack paths gives more possible ways for an attacker to violate the security policy of the network. However the effort put by an attacker at every path is not illustrated by this metric. This is the main drawback of this metric. This metric is unreliable and overly sensitive.

2.2.3. Mean of path lengths metric (MPL)

The MPL metric [11] defines the typical path length by measuring the arithmetic mean of all the available path lengths. The typical effort that an attacker can spend to violate the security policies of a network is revealed through this metric. The MPL has the capability to acquire the changes occurred in the network that decreases or increases the level of security. Let $p_1, p_2, \ldots, p_N$ be the number of paths, the Mean Path Length metric can be derived by performing the division operation between the sum of the lengths of total paths with their count. However the network improvements are not being acquired by this metric. There may be increases or decrease in the mean attack path length with the increases or decrease in the number of vulnerabilities. This criterion increases because the attacker, through the increased vulnerabilities, is provided with more critical routes towards the target.

3. Extended metrics

Though there are so many advantages with the above mentioned security metrics, if they are used in an isolated fashion, they lead to some misleading decisions. The major drawback of shortest path metric is its too coarse nature. The major drawback of the number of path metric is it can't reveal the effort of an attacker that can put to compromise the nodes. Simultaneously the MPL metric can't detect the changes that won't affect the changes in the mean path length. Hence the combined utilization of these metrics

results in a comprehensive strategy and results in better security analysis. In this section along with the three metrics one more metric is derived by considering the shortest path metric, named as number of shortest path metric. In this section, a complimentary set of metrics are also introduced by which an efficient security analysis can be carried out by a security engineer over a network. The metrics we propose are the following: the number of shortest path (NSP), the Normalized Mean of Path Lengths (NMPL), the Standard Deviation of Path Lengths (SDPL), the Mode of Path Lengths (MoPL), and the Median of Path Lengths (MePL) [3].

3.1. Number of shortest path metric (NSP)

In the case of network topology, the shortest path can be found in two ways, one is based on number of hops and another is based on distance. The shortest path metric represents that the minimum effort an attacker can put to compromise. The attacker can compromise the network by simply compromising the number of intermediate nodes through a minimum effort at each and every node. This reflects the number of shortest paths based on the number of hops. In the case of network, there exists more number of shortest paths which are having fewer hops. In that case, the main problem is selecting the shortest path. To overcome this problem, the NSP considers the distance of the entire path. The NSP selects the as a shortest path which is having minimum distance. Let $p_1, p_2, \cdots, p_N$ be the number of paths, the NSP initially measures the number of shortest paths based on the number of hops. Then it selects the final shortest path which is having minimum distance among the selected shortest paths.

3.2. Normalized mean of path lengths metric (NMPL)

This NMPL is obtained by dividing the MPL with the total number of paths. This metric helps in the detection of the occurred security degradations and also the improvements. Along with this, this metric also helps in the interpretation of two different network topologies with different number of paths. In the networks comparison, the network with less NMPL value is declared as less secure.

3.3. Standard deviation of path lengths metric (SDPL)

The SDPL is evaluated by adding and then subtracting the mean of the path lengths. It gives a range of distinctive attack path lengths. These distinct path lengths have lengths that are within one standard deviation of the MPL. The main objective of this metric is to find attacks paths of interest.

3.4. Mode of path lengths metric (MoPL)

The attack paths on which most of the times attacks occur is obtained by this metric, MoPL. Further it can also be illustrated as the metric to find the path on which frequent attacks happens. A likely amount of effort that an attacker can put is obtained through this Mode of Path Lengths metric. Unlike the MPL metric which was a dynamic metric, this metric is not changes dynamically based on the network security status.

3.5. Median of path lengths metric (MePL)

The MePL is obtained by deriving the middle value of all the available path lengths. This metric is more advantageous. Since the path lengths may get skewed, the conventional MPL cannot acquire those changes and this MePL can acquire those changes effectively. A path having very small length followed by a path having a very large path length can be biased in the MPL in the network. A security engineer can analyses the variations in the path lengths through this MePL by observing the closeness of the mean attack path length to the middle of all available attack path lengths. It also helps for a security engineer in the provision of guidance to detect the network hardening efforts.

4. Realization

Based on the above derived metrics the security of network topology can be determined. To do this, this work considered two different topologies of a single network. The realization an [13], [14] is done through the random network with same number of nodes. The complete realization of this work is shown in this section. For this purpose two random network topologies are created and the above mentioned metrics are evaluated by choosing a common source and destination node pair. Finally, a comparison is carried out between the measured metrics to evaluate the security. The results obtained are as illustrated below.

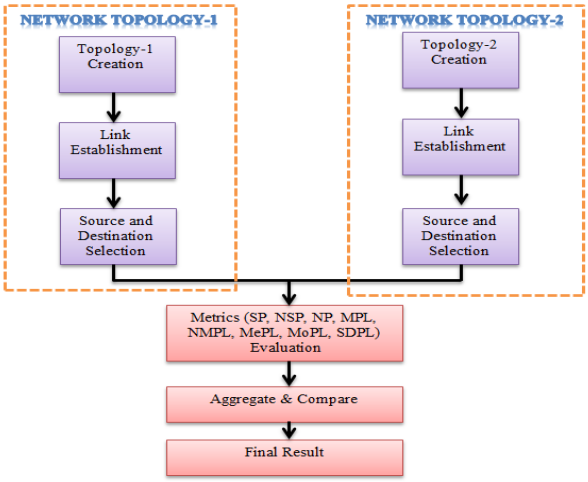


Fig. 2: Flow of Proposed Metric Based Security Evaluation.

4.1. Results of Network Topology 1

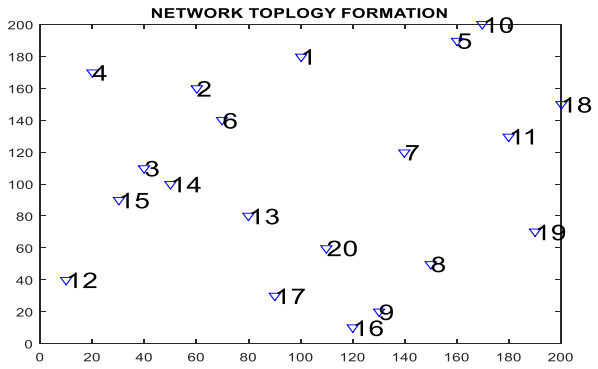


Fig. 3: Random Network Topology Realizing Network Topology 1 Architecture.

Fig.3 shows a network having 20 nodes. In this network, the nodes are created randomly, thus the network topology changes randomly every time. The network topology is realized here by considering the vulnerabilities and conditions as nodes. The above figure gives a realization for the architecture of network topology 1.

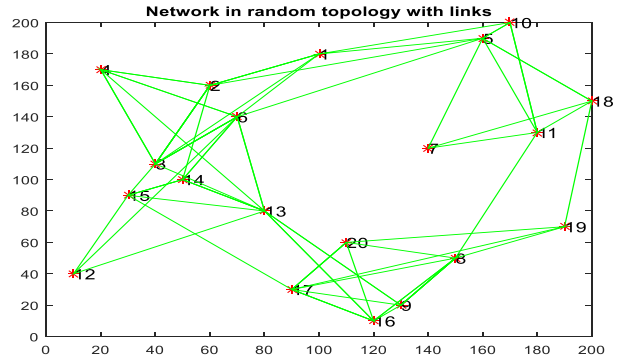
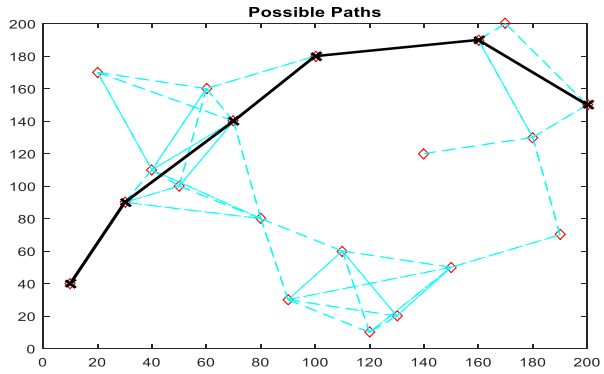


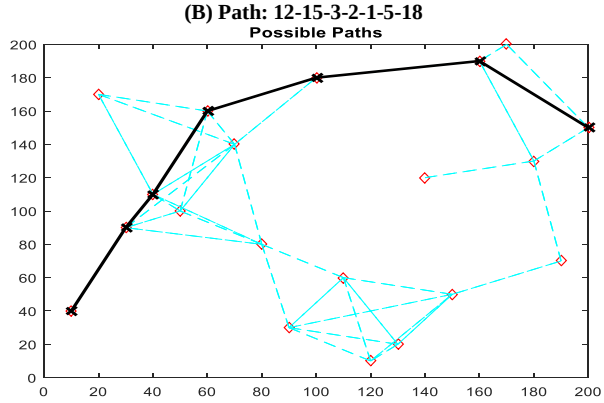
Fig. 4: Random Links Established between All the Nodes in the Network.

Fig.4 represents the possible links established between all nodes. In the above figure, there exists a link between every two nodes. The edges or links are considered as relationships between the vulnerabilities and conditions. For every node there exists a post node and pre node, considered as post condition and precondition. An edge going from a vulnerability node to a condition node shows that the condition node is a post condition of the vulnerability. Multiple post condition nodes for vulnerability are to be interpreted as a disjunction of post conditions. Multiple precondition nodes for vulnerability are to be interpreted as a conjunction of preconditions. Finally, Fig.4 realizes the network topology 1 by considering the vulnerabilities and conditions and their relationships.

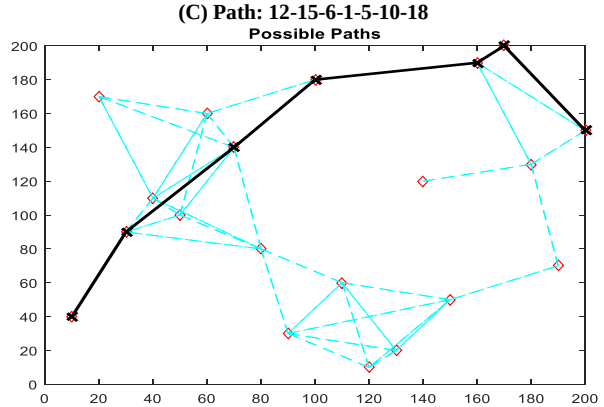
(A) Path: 12-15-6-1-5-18



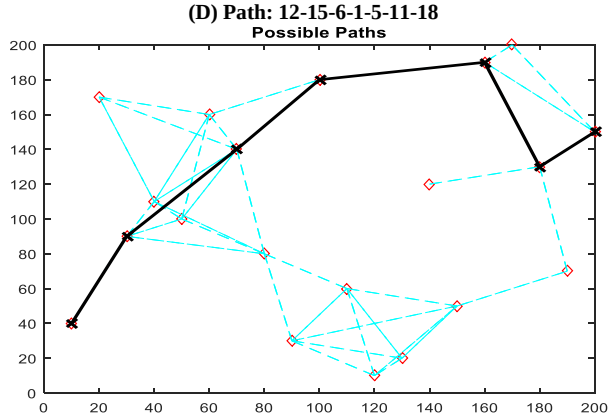
(B) Path: 12-15-3-2-1-5-18



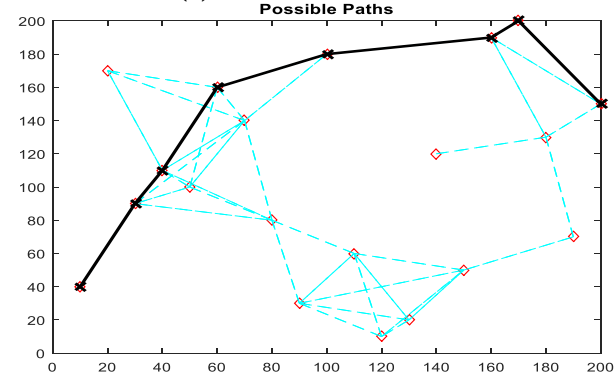
(C) Path: 12-15-6-1-5-10-18



(D) Path: 12-15-6-1-5-11-18



(E) Path: 12-15-3-2-1-5-10-18



(F) Path: 12-15-3-2-1-5-11-18

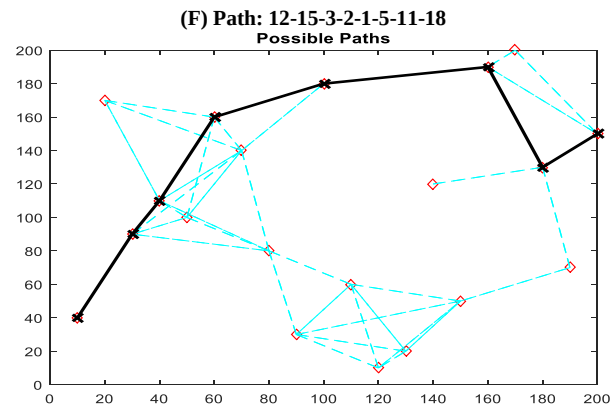


Fig. 5: Number of Possible Available Paths (NP) between Source Node (12) and Destination Node (18).

Path: 12-15-6-1-5-18

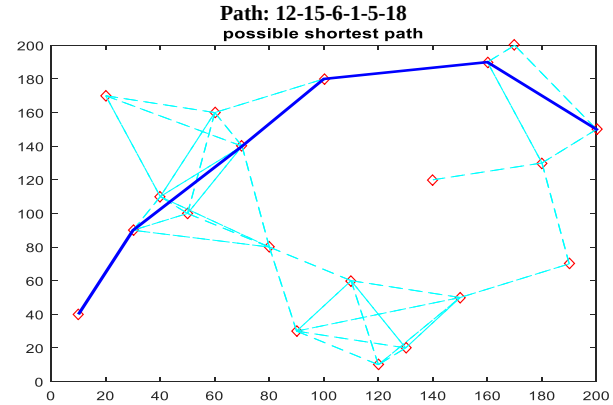


Fig. 6: The Number of Possible Shortest Paths (NSP) between Source Node (12) and Destination Node (18).

Fig.5. represents the total number of availae paths for a given source (12) and destination (18) pair. Fig.6 represents the number of available shortest paths among the total number of available paths based on the hop count. In the above figure, it is observed

that there are totally four shortets paths. Then from the four shortest paths, we need to find an optimal shortets pah which is having less distance which represents the minimum effort can be put by an attacket to compromise the network.

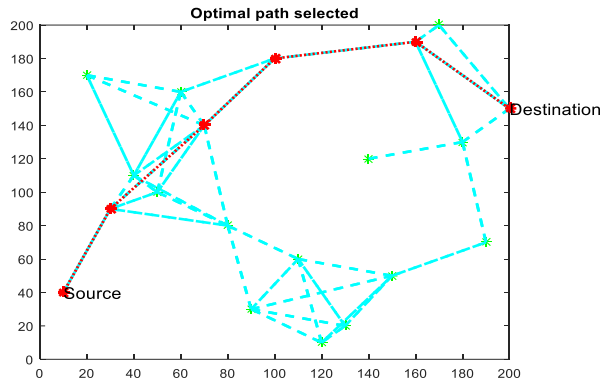


Fig. 7: The Optimal Shortest Path.

Fig.7 represents the optimal path through which an attacker can attack on the network by using minimum effort. As the length of shortest path is more, the network topology is said to be more secure. From the above graphs, the all derived metrics are evaluated and are resented in the Table.1. Table.1 represents the shortest path metric value, number of path metric value, number of shortest path metric value, mean of path length metric value, normalized mean of the path length matric value, median of path length metric value, mode of path length matric value and finally the standard deviation path length matric value of network topology 1, as shown in fig. 3.

Table 1: Metrics of Network Topology 1

Metric	Value
Number of nodes	20
Source node	12
Destination node	18
NP	6
NSP	1
SP	286
MPL	305.8333
NMPL	50.9722
SDPL	15.7252
MePL	304.500
MoPL	0

4.2. Results of network topology 2

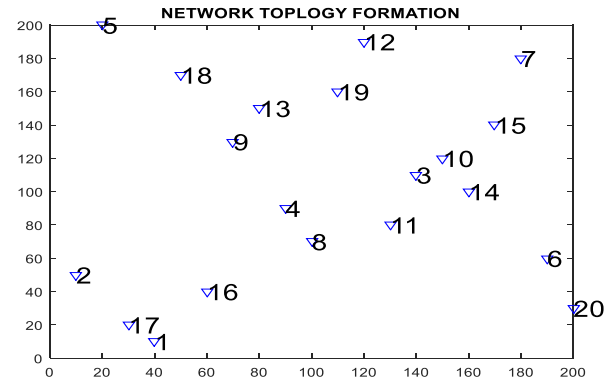


Fig. 8: Random Network Topology Realizing Network Topology 2 Architecture.

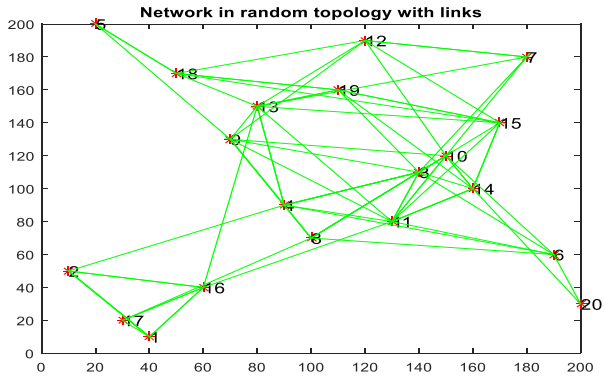
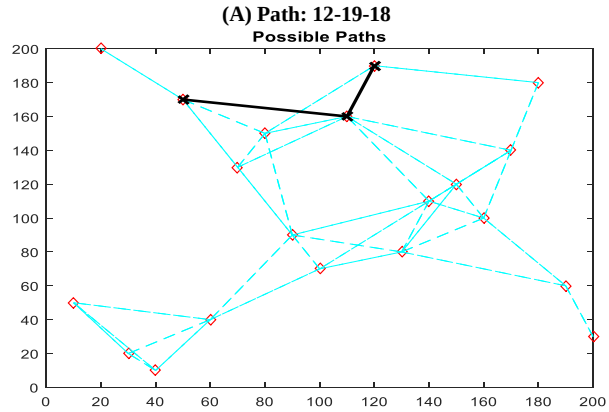
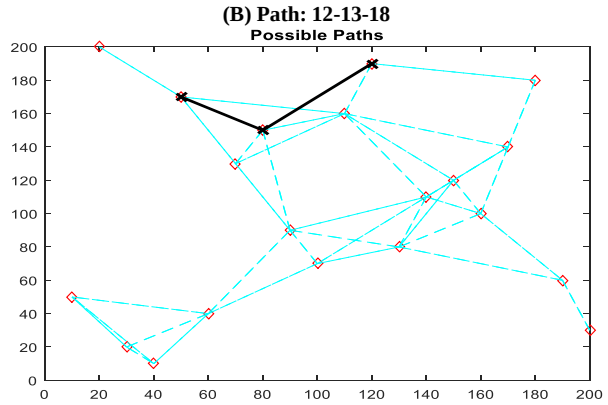
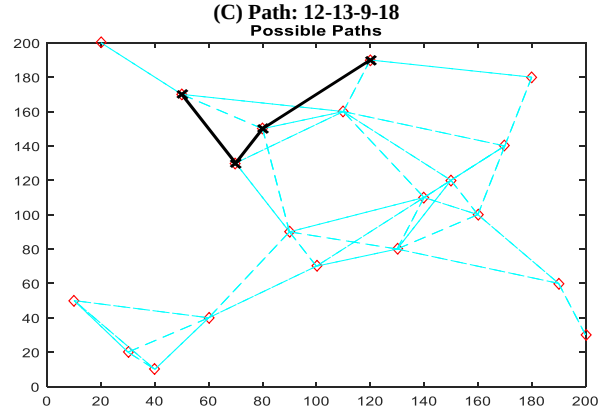


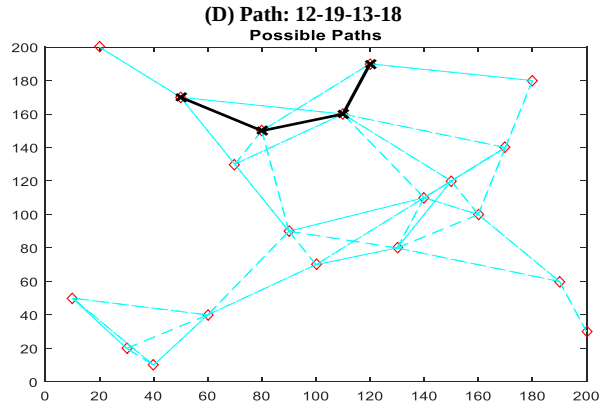
Fig. 9: Random Links Established Between All the Nodes in the Network.

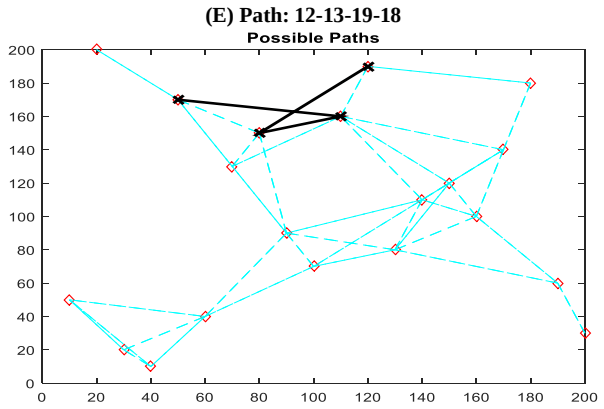
Figure.8 gives a realization for the architecture of network topology 2 and Fig.9. realizes the network topology 2 by considering the vulnerabilities and conditions and their relationships.











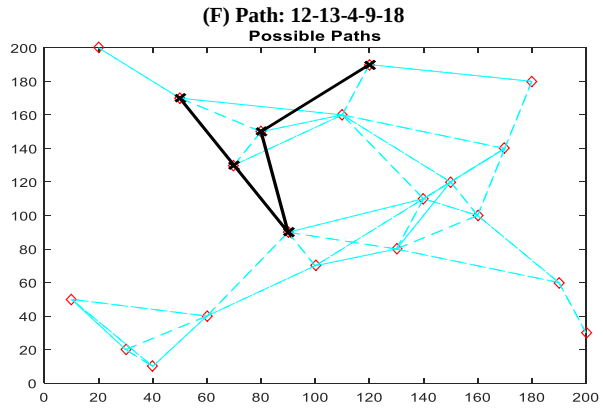
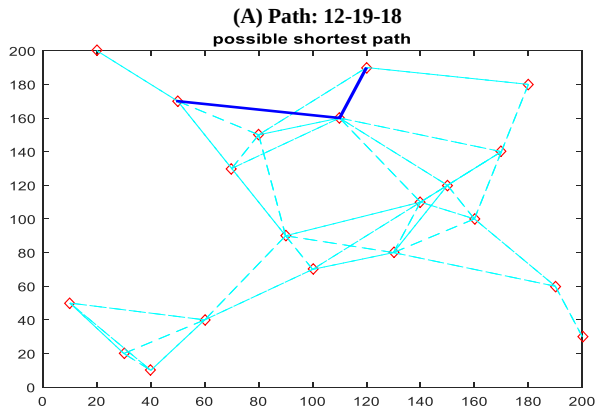


Fig. 10: Number of Possible Available Paths (NP) between Source Node (9) and Destination Node (20).



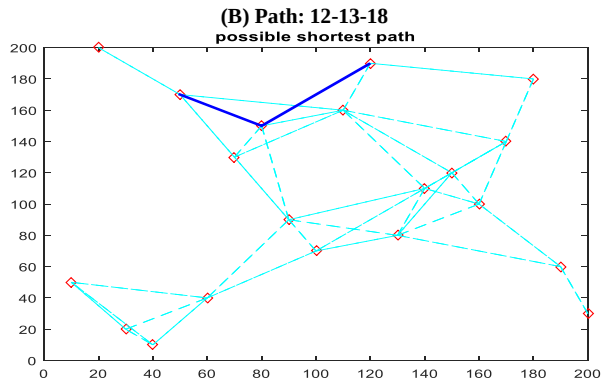


Fig. 11: The Number of Possible Shortest Paths (NSP) between Source Node (12) and Destination Node (18).

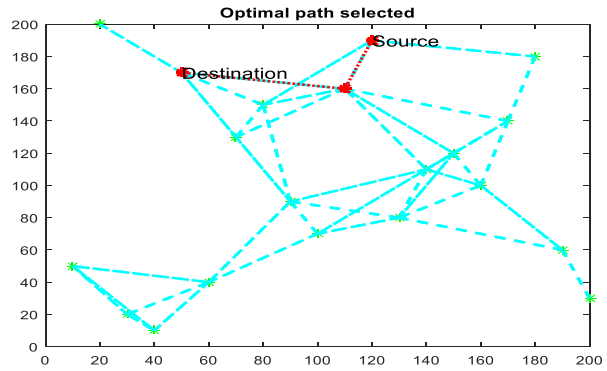


Fig. 12: The Optimal Shortest Path.

Fig.10. represents the total number of availae paths for a given source (12) and destination (18) pair in network topology 2. Fig.12 represents the optimal path through which an attacker can attack on the network by using minimum effort. As the length of shortest path is more, the network is said to be more secure. From the above graphs, the all derived metrics are evaluated and are resented in the table.2. Table.2 represents the shortest path metric value, number of path metric value, number of shortest path metric value, mean of path length metric value, normalized mean of the path length matric value, median of path length metric value, mode of path length matric value and finally the standard deviation path length matric value of network topology 2 shown in fig.8.

Finally, comparison is carried out between the metrics of network topology (NT)-1 and network topology (NT)- 2. Initially, the all developed metrics categorized as decisive and assistive. SP, NP, NSP and NMPL are declared as decision metrics and the remaining metrics are declared as assistive metrics. During the comparison of NT-1 and NT-2 through decision metrics, assistive metrics gives an external assistance. For a comparison based on SP, the MoPL and SDPL gives assistance. For NP based comparison, MePL and SDPL gives the assistance. For NSP based comparison, the MePL and MoPL gives assistance.

Table 2: Metrics of Network Topology 2

Metric	Value
Number of nodes	20
Source node	12
Destination node	18
NP	6
NSP	2
SP	3
MPL	128
NMPL	21.3333
SDPL	45.0200
MePL	112
MoPL	93, 93

Finally for NMPL based comparison, MePL, MoPL and SDPL gives assistance. According to the shortest path metric, a network

which needs ore security will be having high shortest path metric value. As the shortest path metric value is high, the effort should be more and thus attacker can't compromise the network. From the table.1 and table.2, the SP of NT-1 is 286 and the SP of NT-2 is 3. Thus NT-1 is more secure compared to NT-2. Next the comparison is carried out with respect to Number of path metric. according to the NP metric, the graph which is having high NP metric value will be less secure, because if there is more number of paths, the attacker will attack in any way. From the table.1 and table.2, the NP of NT-1 is 6 and the NP of NT-2 is 6, thus both have equal level of security. Next the comparison is according to number of shortest path metric value. This is analogous to NP only. Thus from table.1, the NSP of NT-1 is 1 and from table.2, the NSP of NT-2 is 2. So NT-1 is more secure compared to NT-2. Next metric is Normalized mean path length metric. According to NMPL, the graph which is having less NMPL value seems to be less secure. From the table.1, the NMPL of NT-1 is 50.9722 and from table.2, the NMPL of NT-2 is 21.3333. So the NT1 is more secure compared to NT-2. Finally, the NT-1 is obtained more credits compared to NT-2, thus NT-1 is more secure compared to NT-2.

5. Conclusion & future scope

In this paper, the security analysis is carried out through the path based analysis metrics. The path based metrics here tried to detect the all possible ways that an attacker tries to compromise the network by knowing the characteristics of path such as length, count and their subsequences such as mean, standard deviation, mode and Median. A decisive strategy is formulated here to decide the network which was more secure based on these metrics. Two random networks are created with varying node positions and all these metrics are measured for every network and then a comparative analysis sis carried out between them to finalize a secure network topology and the network which obtained more credits is declared as a more secure.

References

[1] F. Akyildiz, Weilian Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks", IEEE Communications Magazine, Vol. 40, No. 8, pp. 102-114, August 2002. https://doi.org/10.1109/MCOM.2002.1024422.

[2] Yanli Yu, Keqiu Li, Wanlei Zhou, and Ping Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures", Journal of Network and Computer Applications, Vol. 35, No. 3, pp. 867-880, May 2012. https://doi.org/10.1016/j.jnca.2011.03.005.

[3] Nwokedi Idika and Bharat Bhargava, "Extending Attack Graph-Based Security Metrics and Aggregating Their Application", IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 1, pp.75-85, February 2012. https://doi.org/10.1109/TDSC.2010.61.

[4] Richard Lippmann, Kyle Ingols, Chris Scott, Keith Piwowarski, Kendra Kratkiewicz, Mike Artz, and Robert Cunningham, "Validating and Restoring Defense in Depth Using Attack Graphs," In: Proc. of Conf. on Military Communications, Washington, DC, USA, pp.1-10, October 2006. https://doi.org/10.1109/MILCOM.2006.302434.

[5] Joseph Pamula, Sushil Jajodia, Paul Ammann, and Vipin Swarup, "A Weakest-Adversary Security Metric for Network Configuration Security Analysis", In: Proc. of Second ACM Workshop on Quality of Protection, Alexandria, Virginia, USA, pp. 31-38, October 2006. https://doi.org/10.1145/1179494.1179502.

[6] S. Jha, O. Sheyner, and J. Wing, "Two Formal Analyses of Attack Graphs", In Proc. of 15th IEEE Computer Security Foundations Workshop, Cape Breton, NS, Canada, pp.49 June 2002. https://doi.org/10.1109/CSFW.2002.1021806.

[7] Ram Dantu and Prakash Kolan, "Risk Management Using Behavior Based Bayesian Networks", In: Proc. of Conf. on Intelligence and Security Informatics, University of nor Texas, pp. 115-126, 2005. https://doi.org/10.1007/11427995_10.

[8] Lingyu Wang, Tania Islam, Tao Long, Anup Singhal, and Sushil Jajodia, "An Attack Graph-Based Probabilistic Security Metric", In: Proc. of Conf. on Data and Applications Security and Privacy (DAS '08), London, UK, pp. 283-296, 2008. https://doi.org/10.1007/978-3-540-70567-3_22.

[9] Cynthia Phillips and Laura Painton Swiler, "A Graph-Based System for Network-Vulnerability Analysis", In: Proc. of the 1998 workshop on New security paradigms, Charlottesville, Virginia, USA, pp. 71-79, 1998. https://doi.org/10.1145/310889.310919.

[10] R. Ortalo, Y. Deswarte, and M. Kaaniche, "Experimenting with Quantitative Evaluation Tools for Monitoring Operational Security," IEEE Transactions on Software Engineering, Vol. 25, Issue 5, pp. 633-650, September 1999. https://doi.org/10.1109/32.815323.

[11] Wei Li and Rayford Vaughn, "Cluster Security Research Involving the Modeling of Network Exploitations Using Exploitation Graphs", In: Proc. of Sixth IEEE International Symposium on Cluster Computing and Grid, Singapore, pp.1-11, May 2006. https://doi.org/10.1109/CCGRID.2006.1630921.

[12] Lingyu Wang, Anoop Singhal, and Sushil Jajodia, "Measuring Overall Security of Network Configurations Using Attack Graphs", In: Proc. of Conf. on Data and Applications Security, Redondo Beach, CA, USA, pp. 98-112, August 2007. https://doi.org/10.1007/978-3-540-73538-0_9.

[13] Kyle Ingols, Richard Lippmann, and Keith Piwowarski, "Practical Attack Graph Generation for Network Defense", In: Proc. of Conf. on Computer Security Applications, Miami Beach, FL, USA, pp. 121-130, December 2006.

[14] S. Noel, M. Jacobs, Pramod Kalapa, and Sushil Jajodia, "Multiple Coordinated Views for Network Attack Graphs", In: Proc. of IEEE Workshop on Visualization for Computer Security, Minneapolis, MN, USA, pp. 99-106, November 2005.

[15] Dr. Seetaiah Kilaru, Hari Kishore K, Sravani T, Anvesh Chowdary L, Balaji T "Review and Analysis of Promising Technologies with Respect to fifth Generation Networks", 2014 First International Conference on Networks & Soft Computing, ISSN:978-1-4799-3486-7/14,pp.270-273,August2014.

[16] Meka Bharadwaj, Hari Kishore "Enhanced Launch-Off-Capture Testing Using BIST Designs" Journal of Engineering and Applied Sciences, ISSN No: 1816-949X, Vol No.12, Issue No.3, page: 636-643, April 2017.

[17] P Bala Gopal, K Hari Kishore, B.Praveen Kittu "An FPGA Implementation of On Chip UART Testing with BIST Techniques", International Journal of Applied Engineering Research, ISSN 0973-4562, Volume 10, Number 14 , pp. 34047-34051, August 2015.

[18] A Murali, K Hari Kishore, D Venkat Reddy "Integrating FPGAs with Trigger Circuitry Core System Insertions for Observability in Debugging Process" Journal of Engineering and Applied Sciences, ISSN No: 1816-949X, Vol No.11, Issue No.12, page: 2643-2650, December 2016.

[19] Mahesh Mudavath, K Hari Kishore, D Venkat Reddy "Design of CMOS RF Front-End of Low Noise Amplifier for LTE System Applications Integrating FPGAs" Asian Journal of Information Technology, ISSN No: 1682-3915, Vol No.15, Issue No.20, page: 4040-4047, December 2016.

[20] N Bala Dastagiri, K Hari Kishore "Novel Design of Low Power Latch Comparator in 45nm for Cardiac Signal Monitoring", International Journal of Control Theory and Applications, ISSN No: 0974-5572, Vol No.9, Issue No.49, page: 117-123, May 2016.

[21] N Bala Gopal, Kakarla Hari Kishore "Reduction of Kickback Noise in Latched Comparators for Cardiac IMDs" Indian Journal of Science and Technology, ISSN No: 0974-6846, Vol No.9, Issue No.43, Page: 1-6, November 2016.

[22] S Nazeer Hussain, K Hari Kishore "Computational Optimization of Placement and Routing using Genetic Algorithm" Indian Journal of Science and Technology, ISSN No: 0974-6846, Vol No.9, Issue No.47, page: 1-4, December 2016.

[23] N.Prathima, K.Hari Kishore, "Design of a Low Power and High Performance Digital Multiplier Using a Novel 8T Adder", International Journal of Engineering Research and Applications, ISSN: 2248-9622, Vol. 3, Issue.1, Jan-Feb., 2013.

[24] S Nazeer Hussain, K Hari Kishore "Computational Optimization of Placement and Routing using Genetic Algorithm" Indian Journal of Science and Technology, ISSN No: 0974-6846, Vol No.9, Issue No.47, page: 1-4, December 2016.

[25] S.V.Manikanthan and T.Padmapriya "Recent Trends In M2m Communications In 4g Networks And Evolution Towards 5g", International Journal of Pure and Applied Mathematics, ISSN NO: 1314-3395, Vol-115, Issue -8, Sep 2017.

[26] T. Padmapriya and V. Saminadan, "Priority based fair resource allocation and Admission Control Technique for Multi-user Multi-class downlink Traffic in LTE-Advanced Networks", International Journal of Advanced Research, vol.5, no.1, pp.1633-1641, January 2017. https://doi.org/10.21474/IJAR01/2929.