IJARIIT
INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume3, Issue5)
Available online at www.ijariit.com

Vulnerability Assessment of Sensor Network Using Multisink Timestamp And Attack Graph Based Metrics

Ms. Priyanka Patil Nagnath
P.G Student M.E Computer Science & Engineering,
Shriram Institute of Eng. & Technology,
Paniv, Maharashtra, India
priyankapatiln49@gmail.com

Prof. Dhainje Prakash B.
Head of CSE Dept.
Shriram Institute of Eng. & Technology,
Paniv, Maharashtra, India.
dhainjeprakash@gmail.com

Abstract —Attack graph security metrics used for providing the security to the network. We proposed mainly three algorithms those are shortest path metrics, Number of paths metrics and mean of path length metrics. These three techniques is mostly used, for example where the earthquakes or volcanos can occur. In our work we are findings the hotspots areas or sensing the hotspot points from the large geographical areas where the volcanos or earthquakes may be occurred in future and these three algorithms providing the security to that area so that we can avoid the volcanos or earthquakes. But attack graph security metrics used for aggregating the result of those three security metrics and provide the more security.

Keywords-Network level security, Multisink, Measurements, Measurement Techniques.

I. INTRODUCTION

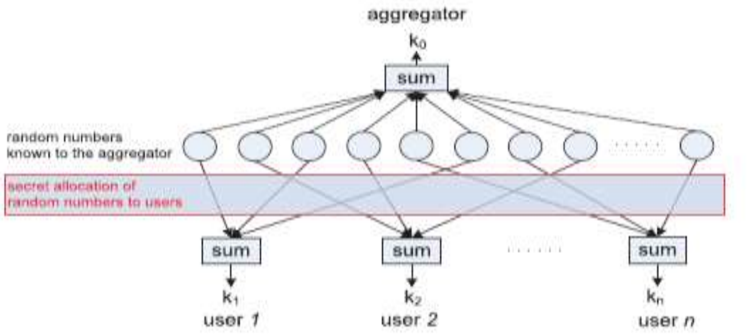
The attack graph is an abstraction that reveals the ways an attacker can leverage vulnerabilities in a network to violate a security policy. When used with attack graph-based security metrics, the attack graph may be used to quantitatively assess security relevant aspects of a network. The Shortest Path metric, the Number of Paths metric, and the Mean of Path Lengths metric are three attack graph-based security metrics that can extract security-relevant information. However, one's usage of these metrics can lead to misleading results. The Shortest Path metric and the Mean of Path Lengths metric fail to adequately account for the number of ways an attacker may violate a security policy. The Number of Paths metric fails to adequately account for the attack effort associated with the attack paths. To overcome these shortcomings, we propose a complimentary suite of attack graph-based security metrics and specify an algorithm for combining the usage of these metrics. We present simulated results that suggest that our approach reaches a conclusion about which of two attack graphs correspond to a network that is most secure in many instances. For example this technique is used where the possibilities of volcanos or earthquakes can occur. For finding the points where the volcanos or earthquakes may be occurred in future. After finding those points these three algorithms provide the security to those hotspots. Attack graph based security metric sis used for aggregating the result of those three security algorithm. In mobile Network it is sometimes necessary for users to share the power to use a cryptosystem. The system secret is divided up into shares and securely stored by the entities forming the distributed cryptosystem. The main advantage of a distributed cryptosystem is that the secret is never computed, reconstructed, or stored in a single location, making the secret more difficult to compromise. Investigations within the fields of threshold group-oriented aggregated Key schemes, threshold group aggregated Key schemes, Multisink Time Stamp schemes, and Threshold-Multisink Time Stamp schemes resulted in explicitly defining the properties of Threshold-Multisink Time Stamp schemes. Existing System for providing the security to the computer network or for any application is in many applications, a threshold or more shareholders are required to cooperatively generate a digital aggregated Key, in contrast to the conventional single signer. This may also be seen as a distribution of trust since the shareholders must collaborate and contribute equally to produce a valid multiparty aggregated Key. Threshold Multisink Time Stamp schemes combine the properties of threshold group-oriented aggregated Key schemes and Multisink Time Stamp schemes. In the literature, Multisink Time Stamp schemes are also referred to as threshold aggregated Key schemes with traceability. The combined properties guarantee the aggregated Key verifier that at least t members participated in the generation of the group-oriented aggregated Key and that the identities of the signers can be easily established. The majority of the existing Multisink Time Stamp schemes belong to variants of the single signatory, generalized Straw-man aggregated Key extended to a group/multiparty setting. But we Proposed System for security. This project is to propose a new Multisink Time Stamp scheme without a trusted third party (TTP), based on a round optimal, publicly verifiable DKG protocol. The proposed scheme can be easily adapted to incorporate a TTP; a version of the proposed scheme with the assistance of a TTP will therefore not be presented. While the above mentioned security metrics can be useful if used appropriately, if any metric is used in isolation, one may arrive at a misleading conclusion. The Shortest Path metric can be too coarse. The Number of Paths metric does not capture attacker effort. The Mean of Path Lengths metric does not detect changes that do not affect the mean path length. If these metrics are used together, they can give a more comprehensive measure of security. We detail how in Section 5. However, in this section, we propose a complimentary set of metrics to assist a security engineer in determining more relevant properties of the network to determine its security. The metrics we propose are the following: the Normalized Mean of Path Lengths metric, the Standard Deviation of Path Length metric, the Mode of Path Lengths metric, and the Median of Path Lengths metric.

The proposed discrete logarithm-based Multisink Time Stamp scheme is also proactively secure, allowing for DKR to a new access structure and periodic DKU to mitigate attacks from an active/mobile adversary. The proposed discrete logarithm-based Multisink Time Stamp scheme is made proactively secure by periodically updating secret shares and facilitating changes in group membership by allowing an authorized subset of existing group members to redistribute secret shares to a new access structure. The scheme fulfills all the fundamental properties of generic Multisink Time Stamp schemes given in the properties of Multisink Time Stamp and resists attacks to which other similar schemes are subject.

II. RELATED WORK

The efficiency of Multisink Time Stamps may be based on following four criteria-

Straw-Man Construction for Key Generation-


aggregator
k_0
sum
random numbers known to the aggregator
secret allocation of random numbers to users
sum
sum
sum
k_1
user 1
k_2
user 2
k_n
user n

The intuition behind the straw-man construction. The aggregator computes the sum of a set of random numbers as the decryption key. These numbers are secretly allocated to the users, and each user computes the sum of its allocated numbers as the encryption key. The aggregator does not know which random numbers are allocated to each user, and thus does not know any user's key.

Intuition of the straw-man construction. Suppose there are nc random numbers. The aggregator has access to all the numbers, and it computes the sum of these numbers as the decryption key k0. These numbers are divided into n random disjoint subsets, each of size c. These n subsets are assigned to the n users, where each user has access to one subset of numbers. User i compute the sum of the numbers assigned to it as the encryption key ki. Clearly, holds. The aggregator cannot know any user's encryption key because it does not know the mapping between the random numbers and the users. When c is large enough, it is infeasible for the aggregator to guess the numbers assigned to a particular user with a brute-force method. The aggregator's decryption key cannot be revealed by any user because no user knows all the numbers.

Construction

The construction is as follows: Secret Setup. The key dealer generates nc random and different secrets s1snc. It divides these secrets into n random disjoint subsets, with c secrets in each subset. Let S denote the set of all secrets.

Group Public Key Length

The Multisink Time Stamp scheme avoids conspiracy attacks without attaching a random secret to shares. The group public key is dependent on the number of group members, as the aggregated Key verifier needs the individual public values of all group members to compute the subgroup public key that is required to verifying the aggregated Key. Difficulty will be experienced with this scheme when trying to eliminate the need for a trusted authority to distribute the initial group key shares. A robust authentication mechanism is essential for securing a distributed system against active adversaries and central to ensure the traceability of individual Signers. The proposed Multisink Time Stamp scheme uses the long-term private keys of the members, provided by a public key infrastructure, to avoid conspiracy attacks even if colluding members derive or control the group secret. As a result of members including their private keys in their individual aggregated Keys, the public key of the scheme consists of the public key of the subgroup that collaborated to generate the threshold aggregated Key. The public key of the subgroup is a function of the is a function of the long-term public keys of the group members.

Group-Oriented Aggregated Key Size

The main contribution to the communication overhead, post aggregated Key generation, is made by the size of the group aggregated Key. The aggregated Key size of Multisink Time Stamp schemes is bound to be dependent on the threshold parameter. This conclusion is drawn from the traceability property of Multisink Time Stamp schemes, which specifies that any outsider must be able to retrieve the identities of the individual signers from the threshold aggregated Key.

Communication Cost of aggregated key Generation and Verification
In terms of communication cost, the individual and threshold aggregated Key generation mechanisms of all the existing Multisink Time Stamp schemes and the proposed scheme are almost equivalent. Multiparty aggregated Key schemes constructed from Straw-man type (discrete logarithm-based) aggregated Key variants are bound to be interactive. In round one, each participant generates a commitment and in the second round, generates an individual aggregated Key on an arbitrary message. In the third round, participants send their contribution to a combiner or designated clerk which constructs the threshold aggregated Key.

Computational Cost of Aggregated Key Generation and Verification

To make a feasible comparison between the computational cost of the proposed Multisink Time Stamp scheme and similar schemes it is assumed that the system parameters are chosen to yield the same time complexity for exponentiations, multiplications, and summations. Although summations and, in some cases, multiplications contribute to an insignificant fraction of the overall time complexity, these operations are still included for the sake of completeness. Values that remain constant between different aggregated Key generations can be precomputed and are therefore not included in the analysis. The computational cost of the schemes will be given in terms of the minimum members required to collaboratively sign an arbitrary message .The computational overhead that causes the most concern is the number of exponentiations in the individual aggregated Key verification and in Multisink Time Stamp verification, which are anticipated to contribute the bulk of the verification time complexity.

III. GRAPH MATRICS COLLECTION

These three algorithms are used in project

1. Normalized Mean of Path Lengths Metric-
The Normalized Mean of Path Lengths metric is the Mean of Path Lengths metric divided by the Number of Paths metric. The identified shortcomings of the Mean of Path Lengths metric stems from its failure to appropriately take into account the Number of Paths metric. The Normalized Mean of Path Lengths metric addresses this issue by normalizing the Mean of Path Lengths by the number of paths in the attack graph. Through this approach, we can detect fine granular improvements and degradations in network security. Moreover, this metric provides an approach for interpreting two attack graphs that have a different number of attack paths. For instance, if vulnerabilities 15 through 20 are removed from attack graph Gi, the new attack graph would be deemed more secure than the original attack graph by the Normalized Mean of Path Lengths metric. In comparing two attack graphs, the attack graph with the smaller Normalized Mean of Path Lengths metric is deemed less secure. The Mean of Path Lengths metric represents the typical path length by obtaining the arithmetic mean for all path lengths. It gives an expected effort an attacker may expend to violate a network security policy. This metric is relevant because an attacker may not have the same view of the known vulnerabilities as the security engineer. Security policy. The Mean of Path Lengths metric has the ability to capture changes that occur in the network that either increase or decrease security levels. Because this mean value is computed over the entire attack graph, any degradation that results in shorter path lengths will affect the mean path length if no other path increases in length to the degradation.

2. Standard Deviation of Path Lengths Metric-

The Standard Deviation of Path Lengths metric, when added and subtracted from the Mean of Path Length metric, gives a range containing typical attack path lengths. These typical attack path lengths have path lengths that are within one standard deviation of the mean path length. The Standard Deviation of Path Lengths metric may also reveal attack path so interest. If, for instance, a path length is two standard deviations below the Mean of Path Lengths metric, this path may deserve the attention of the security engineer.

3. Mode of Path Lengths Metric

The Mode of Path Lengths metric gives the attack path length that occurs most frequently. This metric represents another meaning of typical. In this context, typical refers to most frequent. If the security engineer is unable to determine the likelihood of an attacker traversing any attack path. The Number of Paths metric is a value that represents the number of ways an attacker can leverage existing dependencies among vulnerabilities to violate a network's security policy. The Number of Paths metric is one that is designed to express how exposed a network is to attack. This security metric expresses the number of attack paths that exist within a given attack graph.

Attack graph-based security metrics-

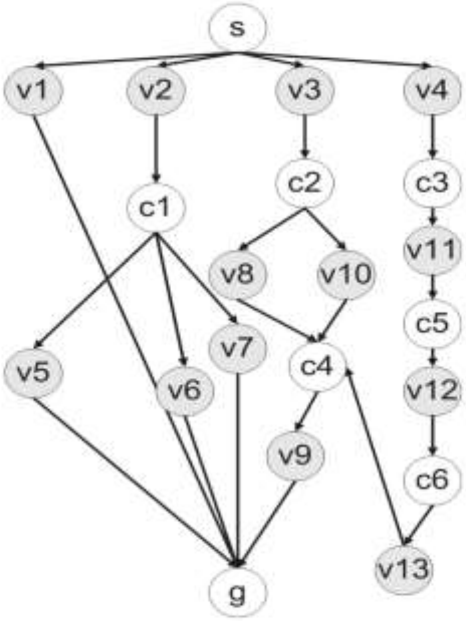


Fig. Attack graph Gj with vaulnarabites at 1 to13

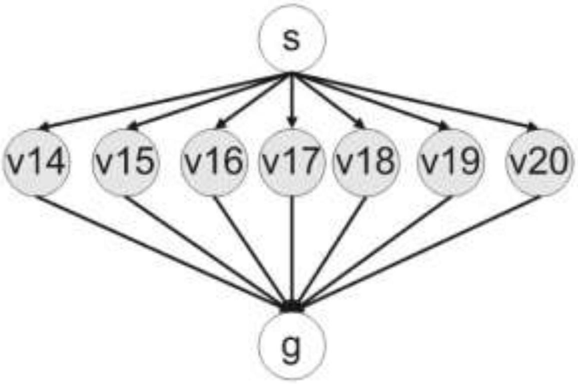


Fig. Attack graph Gi with vaulnarabites at 14 to20

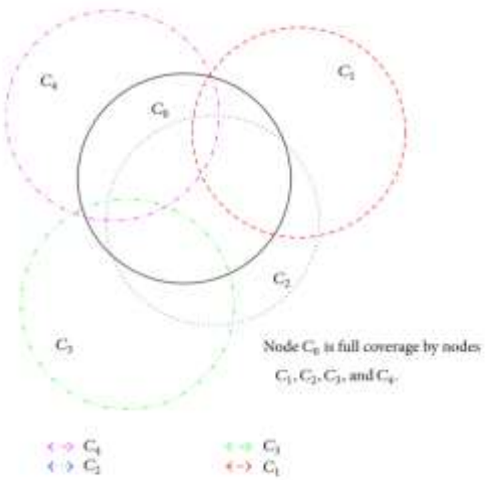
Network configurations Si and Sj that a security engineer is considering deploying, and the security engineer wants to assess the security of these two systems to determine which network to deploy. Let the attack graphs Gi and Gj in Figs. 2 and 3 correspond to the attack graphs generated for Si and Sj, respectively. Thus, when we state Gi is less secure than Gj , then Si is less secure than Sj. These examples were carefully chosen to obviate the differences in security between the two underlying networks. This choice is essential because it illuminates the expected outcome of comparing the two attack graphs: Gj is more secure than Gi.

IV. RESULT ANALYSIS

Mathematical Model for Coverage Guarantee Protocol

One of the main approaches of the proposed scheme is the coverage calculation to guarantee all events an area interested. Sensors will be scheduled for WORKING mode or SLEEPING mode based on the minimum set of nodes to achieve full coverage. The guaranteed coverage calculation must satisfy three conditions:

Assume that all sensor nodes have the same communication range and sensing range. The coverage calculation is


C_4
C_0
C_1
C_2
C_3
Node C_0 is full coverage by nodes
C_1, C_2, C_3, and C_4.
C_4
C_2
C_3
C_1

C0 node is covered perimeter by nodes C4, C1, C2, and C3. In this case one node passes the perimeter test but the perimeter test has a limitation about the coverage guarantee.

At least one node in the perimeter test list that can cover the center

$$d(C2,C0) < r_s$$

The general condition for the center test is defined

$$\ni d[(C_I,C_A)< r_s] ,i=(0,\ldots..,n) , i \neq A$$

Node CO passes the condition of the center test but cannot be fully covered by C2, C3, C4, and to overcome this problem, there is the distance test. The coverage of neighbors must sufficiently close to ensure full coverage. In some cases, there may not be an uncovered area within the sensing region. In the center test, the best center node must reach all perimeter test nodes to achieve full coverage.

$$d(C_2 , C_i) < d(C_2 ,C_0) + r_s \quad \text{Where } i= 1,3,4.$$

The condition for the distance test is defined as

$$d(C_2 , C_i) < d(C_A , C_0) + r_{s,}$$

$$i= (0,\ldots,n), i\neq A,0.$$

The volcano or earthquakes is occurred at some places in large geographical area then we want to find out points where volcanos or earthquakes may occur.so that this project is to find out the hotspots from the cluster i.e from large area. For that purpose sensor is used or sensor senses us that hotspots. Sensor senses these points where the volcano may occur in the future. After finding that hotspots we can provide the security to that area.so that we can avoid the volcanos which are occurred. For the security purpose we use three algorithms those are shortest path metrics, Number of paths metrics and mean of path length metrics. These three algorithms providing the security to that area so that we can avoid the volcanos or earthquakes. But attack graph security metrics used for aggregating the result of those three security metrics and provide the more security.

CONCLUSION

The main aim of this project is to find out the points where the volcanos or earthquakes may occur in future and provide the security to that point. To introduce a secure Multisink Time Stamp scheme. To reach this objective, the secure and optimally efficient Straw-man type aggregated Key variant, GES, was extended to a multiparty setting to yield a Multisink Time Stamp scheme, which provides a guaranteed traceability property. The proposed Multisink Time Stamp scheme was shown to satisfy all of the specified security requirements and fulfills the stronger break-resistant property. The Multisink Time Stamp aggregated Key scheme thus remains secure, even if the threshold cryptosystem has been broken, i.e., the group secret or individual secret shares are known or controlled by an adversary. The efficiency analysis showed that the proposed Multisink Time Stamp scheme outperforms other existing schemes and is optimal in terms of exponentiations with respect to threshold aggregated Key verification and near optimal for individual aggregated Key verification, while providing break resistance.

ACKNOLEDGEMENT

The proposed system is based on IEEE Transaction paper under the title An Authentication Protocol for Clustered Wireless Sensor Networks published in IEEE TRANSACTIONS in computer science volume 8,no 3,March / April 2017

REFERENCES

[1] Joel Joy Manjaly and J Sandeep An Authentication Protocol for Clustered Wireless Sensor Networks International Journal of Advanced Research in Computer Science Volume 8, No. 3, March – April 2017

[2] Nwokedi Idika,Bharat Bhargava, Fellow, ” Extending Attack Graph-Based Security Metrics and Aggregating Their Application”,published in IEEE transactions on dependable secure computing,vol.9,no.1,january/february 2012.

[3]V.Thiruppathy Kesavan, S. Radhakrishnan “Multiple Secret Keys based Security for Wireless Sensor Networks International Journal of Communication Networks and Information Security (IJCNIS) Vol. 4, No. 1, April 2012.

[4]. N. Idika, B. Marshall, and B.Bhargava, “Maximizing Security given a Limited Budget,” Proc. TAPIA ’09: Richard Tapia Celebration of Diversity in Computing, Apr. 2009.

[5]. R. Lippmann, K. Ingols, C. Scott, K. Piwowarski, K. Kratkiewicz, M. Artz, and R. Cunningham, “Validating and Restoring Defense in Depth Using Attack Graphs,” Proc. Military Communications Conf., Oct. 2006.

[6]. J.Pamula, S. Jajodia, P. Ammann, and V. Swarup, “A Weakest-Adversary Security Metric for Network Configuration Security Analysis,” Proc. Second ACM Workshop Quality of Protection, pp. 31-38, 2006.

[7]. S. Jha, O. Sheyner, and J. Wing, “Two Formal Analyses of Attack Graphs,” Proc. 15th IEEE Computer Security Foundations Workshop, June 2002.

[8] L. Wang, T. Islam, T. Long, A. Singhal, and S. Jajodia, “An Attack Graph-Based Probabilistic Security Metric,” Proc. Data and Applications Security (DAS ’08), pp. 283-296, 2008. [9] Y. Desmedt, “Society and Group Oriented Cryptography: A New Concept,” Proc. Advances in Cryptology—CRYPTO ’87, 1987.

[10] Y. Desmedt, “Threshold Cryptography,” European Trans. Telecomm., vol. 5, no. 4, pp. 449-457, 1994.

[11] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin, “Secure Distributed Key Generation for Discrete-Log Based Cryptosystems,” Proc. Advances in Cryptology—EUROCRYPT ’99, May 1999.

[12] C.-M. Li, T. Hwang, and N.-Y. Lee, “Threshold-Multisink Time Stamp Schemes where Suspected Forgery Implies Traceability of Adversarial Shareholders,” Proc. Advances in Cryptology—EUROCRYPT ’94, May 1994.

[13] A. Boldyreva, “Threshold Aggregated Keys, Multisink Time Stamps and Blind Aggregated Keys Based on the Gap-Diffie-Hellman-Group Aggregated Key Scheme,” Proc. Public Key Cryptography—PKC ’03, 2003.

[14] C.-T. Wang, C.-H. Lin, and C.-C. Chang, “Threshold Aggregated Key Schemes with Traceable Signers in Group Communications,” Computer Comm., vol. 21, no. 8, pp. 771-776, 1998.

[15] W.-B. Lee and C.-C. Chang, “(t, n) Threshold Digital Aggregated Key with Traceability Property,” J. Information Science and Eng., vol. 15, no. 5, pp. 669-678, 1999.

[16] Z.-C. Li, J.-M. Zhang, J. Luo, W. Song, and Y.-Q. Dai, “Group- Oriented (t, n) Threshold Digital Aggregated Key Schemes with Traceable Signers,” Proc. Second Int’l Symp. Topics in Electronic Commerce (ISEC ’01), Apr.