Adversarial Modeling in WSN and its Application in Key Distribution

Rohit Bathla\textsuperscript{1}, Priyanka Ahlawat\textsuperscript{2}
National Institute of Technology, Kurukshetra (India)\textsuperscript{1,2}
rohitbathla2005@gmail.com, priyankaahlawat@nitkkr.ac.in

Abstract. Wireless sensor network (WSN) is the interconnection of very small sensors placed in hostile environments. It results in physically node capturing of a node. These further decreases the performance of key management scheme as number of captured nodes increases. In the paper, we approach the issue of node capturing from adversary view. Adversary is considered more intelligent and aims to capture less nodes with maximum destructiveness in the network. This reduces energy capturing cost of adversary in launching this attack. The proposed models exploit different vulnerable points in the networks to build a matrix based attack model. These use dominating set of nodes with node path vulnerability value to quantify the probability of network compromise. These also focus on low capturing cost nodes with high destructiveness in the network. Later, it also considers the travelling capturing cost which also be minimized. Thus all factors are used to compute final attack matrix. It is shown that above models have improved performance in damaging the network in terms of energy capturing cost and number of attacking rounds.

Keywords: Node captures attack, attacking rounds, energy capturing cost, wireless sensor networks.

1. Introduction

Wireless sensor network (WSN) consists of very small and less capturing cost, which may disposed over an end area for regularly monitoring [2]. Such networks hold importance in some areas of army and border area of inspection model, satellite information, climate monitoring, technical security, health concern, and disaster arrangement, where integrity, isolation, are of very importance. WSN more applied to flood discovery, traffic monitoring, attack disclosure, and marine monitoring the systems, over smart hospitals, crime detection, environment monitoring.[4] Nodes are mainly very less hardware capturing cost segments with critical constraints power, memory with information sources. Thus, the nodes has to build and manage one and many hop point to point network connectivity.[12] The node capture attack removes sensor nodes for compromising network and deploy them to produce many attacks. Adversary can transform the data, program and redeployes in the environment of these malicious nodes. [15].

The contribution of our work can be categorized as follows:

(1) We point that the node capturing attack can mould into a graph which shows the connection within capturing the node and compromise the path. Then variables like the dominating set of nodes, path vulnerability, path compromise ratio, capturing cost, and energy of node, travelling cost are defined, which further analyze relationships between these paths and nodes. We suggest three
attacking models that maximizes the node capture effect on the network with a lower number of rounds and with minimum capturing cost.

(2) On the basis of our proposal, we design a node capture attack into an independent dominating set of nodes problem and establish a relationship between dominant node and number of paths for enhancing the attack efficiency while reduce the capturing cost and travelling cost.

(3) We have proposed three attacking models namely dominating node attack (DNA), dominating node travelling attack (DNTA) and dominating node path attack (DNPA) and compare their performance in terms of total energy capturing cost, node capturing cost, travelling cost and path compromise ratio in terms of rounds in capture the whole network.

(4) We simulate to examine the efficiency of our algorithms in terms of attacking rounds and capturing cost of energy nodes in compromising the network.

(5) We propose, examine, and compare our scheme with random schemes and maximum traffic attack (MTA) to justify our proposed scheme.

Wireless sensor network is a distributed sensor wireless ad-hoc network. It can be defined as the self-configured and infrastructure-less wireless networks to monitor physical or environmental conditions namely, sound, temperature, vibration, environmental pollution, various monitoring domains through which data can be observed and analysed. Base station acts like interface between users and the network. One can retrieve crucial information from the network by using specific queries and results can be gathered from the base or sink. Currently, these types of network are in their initial stages only of being deployed to real world time. But in next few years one could find this technology being used in various domains throughout the world. Security is the biggest challenge for WSN from its various issues. Due to its exposure to outer environment, it is prone to various kinds of physical attacks by the intruder. Among various attacks in wireless sensor network, node capture attack is a serious attack through which an intruder can performs various operations on the network and can easily compromise the entire network. Node captures attacks one of the hazardous attack in WSNs. In this, the attacker physically captures the sensor node by gaining access to cryptographic keys and vital information of user. There are various node capturing Attacks such as random attack (RA) where nodes are captured independently of each other. In every round, the intruder selects a vertex to be captured.

Another one is maximum Key Attack (MKA). In this kind of attack, in every round, nodes with highest number of keys are compromised. So, even if the node is not belonging to any route, then also, it is likely to be confined if it has if it has maximum number of keys and Another one is maximum link Attack (MLA) where with every round, nodes having highest number of links are compromised. Also, even if the node does not belong to any route, then also it is likely to be captured.

But there were major drawbacks too, since the attacks mentioned above were not efficient enough and they had some major issues, due to which the attack efficiency of these attacks was low. Some of these issues were like attacking efficiency of node capture attack is very low as it tries and aims to capture the maximum amount of nodes in a network. Also susceptibility is defined as a number, and it cannot specifically describe the level of destruction in WSN. The main problem with these types of attacks is that it focuses only on single criteria thus not providing multi objective so as to achieve lowest cost, maximum keys etc. So an attack was needed which have these multiple objectives like large node contribution, least resource.
2. Research Work

We study that WSN have micro devices that are very ease to capture by the adversary. In attacks, the adversary captures node with extracts the data from the memories, and compromise security. The paper shows, the approach of WSN security mechanism from an attackers view and design a low capturing cost and effective procedure to signify nodes in a WSN in least time with very least capturing cost. Attacker should choose next node based on the network topology. Reason that this identity of such is an NP Hard problem. In the paper, they work to convert the issue into covering problems and design a greedy algorithm to find less capturing cost node capturing attacking algorithm [1]. The concept of networks made viable with the mechanical systems, wireless communications, and digital concepts. In this, the tasks of sensing and sensing potential networks are explored, and a review of influence factors sensor networks is provided. The algorithms developed for each layer are explored. The realization of sensor networks is also discussed.[2].

The key management scheme is designed for the well-known workings of the wireless sensor network are very important. Critically factor that influences the performance security are discussed. The paper takes the problem of node capturing from an attacker point of view point of attacker in which the adversary explores the various vulnerabilities to design a capturing cost effective matrix. The network designer also design a attack matrix by identifying a proper subset of the critical nodes with a compromise key method to give a key dominant rank to the nodes of such a network and select them. The hash chaining mechanism being used for the improvement in the security as rekeying of the scheme. The performance is measure with other methods, and thus gives the improved resilience in order capturing node, hash computations decreased, compromise probability for proxy nodes also reduced with a revoked link [4]. Discussion of these physical capture node attack with an point of adversarial view. Adversary smartly captures these nodes and takes cryptographic data to affect the reliability and security of the node. A hybrid method is design for this path vulnerability matrix with that efficiency to attack is increased, and reduced expenditure in resource capturing cost. That sort of running application, capturing cost of capturing, articulation point, and path length. The result matrix is examined with old strategies in order of the number attacking rounds, capturing cost and traffic compromised. The performance validated by number of path compromise, path length, and route ratio [5].

Connected set of dominating nodes worked as backbone for a WSN. There is not any fixed infrastructure in wireless sensor networks. With help of this approach, routing becomes easy and can adjust the network topology conversions. The studied in disk graphs, with the same transmission range [6]. Proposed a model for capture a node attacks in which an attacker gather data of the network with eavesdropping in a wireless network and collect that no messages with information. The attack is a NP Hard problems are discussed with a heuristic approach of algorithm with the decomposition into a number of tasks, the effect thus can be calculated [7]. Optimized node send the message for energy preservation of the network. The connected dominating set gives an effective technique of messages passing. It is an NP-Hard problem. Degree-based algorithm use for dominating set using 2 hop information, which decrease the capturing cost. First, transform our problem to a set cover problem with a hamilton cycle problem, which also a NP Hard. Then, develop a heuristic called MREA to with minimizing resource expenditure. Simulations are conducted, which performs MREA. Results shows that MREA outperform other results in reduce the number of attacking rounds and save the resource expenditure capturing cost [9].

The attacker intelligently captures the nodes and extracts the key of cryptographic from destroying the security privacy, reliability, and integrity of these wireless sensor networks. It suffers from low efficiency and high capturing cost of expenditure. The approach gives a solution that is a matrix oriented method for modeling the working of the attack. [10]. Node capture attacks in wireless sensor networks affect the confidentiality and integrity of extracting the cryptographic keys to eavesdropping the communications. They propose a graph method for the node capture attack on the random key pre-distribution scheme. A full graph is constructed for the compromising relationship within nodes and
links and thus methods of evaluation is introduced. The FGA is proposed to cover the effect of each node so as to decrease the number of attacking rounds and decrease the time of execution. For supporting the effectiveness of FGA in terms of efficiency, optimal algorithms, called opti attack and path cover attack designed [11].

The problem of physical node capturing in WSN and gives a better control method for modeling of node capture attack. With this analysis of keys and linear automated theory, develop a model that effectively describes the behaviour of that network with attack. Optimal control theory method design a response for the network, which provide a network with secure stability[12]. Capturing the node attack is one of the most severe attacks in WSN. Capturing a node physically they can remove all the data saved in it including attacks by creating clones of a node. Hence how fastly an attacker can manage to collect the data of the node and the network gives an efficiency of node capture attack. They proposed the basis for collecting data by an adversary[13]. Confidentiality of data, network reliability, and security are compromised by the node capture attack. In general, term attacking models are designed for network security mechanisms formalizing problem from an attacker view. Paper presents a general attacking model based on attacking backbones of the network, which is assembled based upon a weakly connected dominating set. The main points of these simulations are conducted to explain the effect of infection ratio on network performance. The study of simulation outcomes determined that a more significant infection ratio could decrease the collection of hazarded nodes, improve attacking performance, save support expense, and decrease the attacking rate[14].

In real-world situations and environments, wireless sensor nodes network becomes a powerful technique. From household monitoring to extending up to the significant service are the applications of WSN. As their use involves sending essential data, which needs the challenge to implement protection in WSNs, in which adversaries can easily hazard the network. It is a hazardous attack in WSN. A robust device is necessarily required to improve the detection of node capture attacks. The survey analyzes design detect schemes to produce a unique technique to provide network resilience against node capture attacks[15]. The network of wireless sensor nodes has no infrastructure very much similar to a mobile cellular network. The energy associated with wireless sensor nodes is very much limited, which dangerously changes the entire system. Hence constructing a virtual backbone starts through the right note. In this paper, an algorithm of minimum connecting dominating nodes depends upon various dominating trees is produced. This practical algorithm favors the node about each kernel region, system as the source node, and creates different dominating sub trees in the order. Then connectors are there to connect the two subtrees that are not connected. Lastly, the dominator is cut off to get the final virtual backbone.[16]. A hash chain based key distribution to increase the resilience of network is given in [17].

From the study of different schemes, we observed that different scheme shave been proposed by researchers to provide an effective and efficient Key distribution for WSN. Still how to provide a better trade off between security and efficiency in KMS is still an open research issue. Adversarial modeling can be used to increase the security during a key distribution. In the proposed scheme, we exploit various vulnerable points in a network that can be exploited by adversary and thus, resilience can be further increased.

3. System Model

The model that are used for the proposed scheme are presented in that part. In this section, we present several models and terminologies that support our proposed model. Notations including specifications are given in table number 1. We also present the block diagram for designing our model.

3.1. Network model
Wireless sensor network is represented by a graph in which every node is a sensor node, and links are protected links among the connecting node of system. The node are designed with some energy capturing cost. Wireless sensor network is created using this network model. This model is represented by directed network graph \( G = (N, L) \), where \( N \) is the nodes number and \( L \) is the links number\[1,5\].

3.2. Path model

Paths are established between the source node and sink node inside a network. Paths thus made of various links. If a link is compromise, the whole path gets effected. In WSN, A link \( L_{a,b} \) is consistent and protected if it is encrypted by \( K_{a,b} \) in which information can be sent between \( N_b \) and \( N_b \) without disturbing to other nodes\[5\]. Therefore, the security of the link \( L_{a,b} \) is directly related to the key size of \( K_{a,b} \) i.e. the larger the key size, higher the protection\[5\]. We indicate the set of all the links in WSN by \( L \), where \( L = \{ L_{a,b} | Na \in N, Nb \in N \} \).

3.3. Adversary model

The adversary has bounded potential and run with a effective algorithm before positioning attack inside the network. It effectively utilizes different vulnerabilities points like a dominating set of nodes path vulnerability with path compromise ratio of the network. Further it directs to compromise the network with the very less number of nodes and energy capturing costs. Network have complete knowledge of physical nodes and random energy of node that is used during the establishment of paths between the source and sink.

3.4. Key Assignment modeling

In \[5\] it is explained that the cryptographic keys represent a key group set \( K \) and every sensor node \( Na \in N \) is randomly assigned a subset of keys \( K_{a} \subset K \) from a key group set. Two nodes \( Na \) and \( Nb \), which share a set of keys \( K_{a,b} = K_{a} \cap K_{b} \) and are located in each other transmission range \( r \), can communicate with each other\[1\]. The set of \( K_{a,b} \) is used to encrypt the information which is transferred between \( Na \) and \( Nb \)[1].

Example: \( K_a = \{ K_1, K_2, K_3, K_4 \} \) and \( K_b = \{ K_3, K_4, K_7, K_8 \} \)
Then \( K_{a,b} = K_{a} \cap K_{b} = \{ K_3, K_4 \} \)

| Symbols | Notations |
|---------|-----------|
| \( N \) | Network’s total set of nodes |
| \( n_i \) | Node \( i \)th inside network |
| \( K \) | Key pool of \( K \) keys |
| \( L \) | Total links inside network |
| \( L_{i,j} \) | Link within nodes \( n_i \) and \( n_j \) |
| \( S_n \) | Set of compromised nodes |
| \( S_k \) | Set of compromised keys |

Table 1 Notations and symbols used
4. The Proposed Energy Efficient Attack Model Based on Independent Dominating Set Of Nodes

This section explains the detail of our scheme. The network architect utilizes the performance of nodes to produce our scheme. Network designer recognizes nodes in dominating set and node path vulnerability with path compromise ratio as the most effective attack by the adversary to interrupt the system. Initially, matrix is designed between the nodes, and dominating nodes are calculated by using algorithm 1. It defines how the whole network is connected with these dominating sets of nodes the probability to attack of these node to compromise the whole network. Then the paths between the source node and the sink are calculated by using algorithm 2. Then we calculate the probability of each dominating node in the total path. The node with the highest PCR is selected by the adversary to capture the node and further used to compromise the whole network. And thus adversary captures fewer nodes with maximum destructiveness in the network with less energy capturing cost. This reduces the energy capturing cost of the adversary in launching this attack. It exploits different vulnerable points in the networks to build a matrix-based attack model. Our model uses dominating nodes and path vulnerability values to quantify the probability of network compromise. It also focuses on low capturing capturing cost nodes with high destructiveness in the network. Later, it also considers the travelling capturing cost, which also be minimized. Thus all factors are used to compute the final attack matrix. It is shown that the above model has improved performance in damaging the network in terms of energy capturing cost with attacking rounds.

4.1. Calculation of nodes belonging to dominating set

First stage of our proposed program contain the establishments of attack matrix from the viewpoint of the adversary. In this the adversary expected to able to destroy the nodes network with the minimum part of nodes in the system. It employs the various vulnerable points present inside the network to design an attack. Static network is used such that the node are not in the state of modify its state after deployment of the network. Network designer find these various vulnerable points and
average values in an offline fashion. Proposed attacking matrix is calculated in sensor network by the network designer.

4.1.1. Dominating Nodes

A nodes subset \( DS \subseteq G \) is called a dominating set if and only if each node of graph \( G \) is in that \( DS \) or is neighbour with atleast one node in \( DS \). That vertex act like backbone in the whole network and traffic are calculated with these nodes. Thus those nodes become the target of adversary that uses minimum resources utilization to compromise the network. Thus in very less time network can be compromise by capturing these nodes. This set contains the attack value to be captured by the adversary and, thus, makes these nodes vulnerable to our node capture attack. Direct and partial compromise methods are used.

The network is considered as a graph where vertices denote nodes, and the edges represent links. The input to this algorithm is an adjacency matrix that represents a graph. And in the output we get a set of dominating nodes that connect the whole network.

4.1.2. Calculate the path vulnerability ratio of nodes belonging to dominating set

After this, each node that is a part of the dominating set of the system is check for their presence in the paths. How many times a node is in the path gives the value of path compromise ratio between two given nodes is calculated by using algorithm 1. Then a node vulnerability value is calculating after considering the captured capturing cost of a node. Finally, adversary select that node having maximum path vulnerability with minimum energy capturing cost and compromise that node. Further adversary follows the same steps until the whole network is compromised.

After computing the PCR of every node of the network, we calculate its attack coefficient. It is based on PCR value and value of capturing cost of a node. The adversary tend to capture the node with least value of capturing cost and high value of destructiveness. Algorithm 3 computes the attack coefficient of nodes of a network.

| Algorithm 1: To Compute AC\(_i\) of Node and attack model |
|----------------------------------------------------------|
| 1. Find DS of the graph by using Algo1                   |
| 2. Print all path from given source to sink by using    |
| algorithm and count total paths(TP)                     |
| 3. Select each node \( v \in DS \) and count PN, path    |
| number of node in total paths(TP)                       |
| 4. Calculate PCR=PN/TP                                   |
| 5. if \( v,u \in DS \), have same value for PCR         |
| 6. Add CC to PCR, and calculate attack coefficient(AC)  |
| = PCR/CC                                                |
| 7. Select node with highest attack coefficient           |
| 8. Compromise selected node                              |
| 9. if network is not compromise                          |
| 10. Repeat all steps                                     |

5. Performance analysis of proposed scheme

That section gives the comparison of various schemes with the new scheme. The performance is analyzed with a scheme in terms of several rounds that it takes to compromise system and shows
energy capturing cost per rounds with different schemes. The simulation is done in Python. We set the value as 1 for source node (N1) and sink node (N2) and rest of the nodes are having values between [0, 1].

Table 2 Random Capturing cost for each node

| Node id | CC  | Node id | CC  |
|---------|-----|---------|-----|
| N1      | 1.0 | N11     | 0.55|
| N2      | 0.75| N12     | 0.65|
| N3      | 0.35| N13     | 0.85|
| N4      | 0.25| N14     | 0.80|
| N5      | 0.40| N15     | 0.55|
| N6      | 0.55| N16     | 0.70|
| N7      | 0.20| N17     | 0.80|
| N8      | 0.20| N18     | 0.85|
| N9      | 0.30| N19     | 0.90|
| N10     | 0.75| N20     | 1.0 |

We analyze the performance of the proposed attack matrix with the following attack models as under:

Blind attack (BA): In this type of attack, no procedure is used to capture the nodes. The adversary randomly catches the nodes. Usually, BA shows poor performance.

Maximum Traffic attack (MTA): In this attack, the adversary captures the nodes with maximum PCR (path compromise ratio) and the capturing cost of obtaining that node to destroy the network. It does so to break a large number of paths in the system.

Dominating Node attack (DNA): In DNA, the adversary aims to capture those nodes that can be in the dominating set of nodes with the maximum path compromise ratio and less capturing cost. The attacker aims to obtain that node step by step and follow the same procedure to compromise the network completely.

Dominating Node Path attack (DNPA): In DNPA, the adversary aims to capture those nodes that are in the first round of dominating set of nodes. The order to select those nodes to capture attack comes with the maximum path compromise ratio and less capturing cost.

Dominating Node Traveling cost attack (DNTA): In DNTA, the adversary aims to capture those nodes that can be in the dominating set of nodes with the maximum path compromise ratio and less capturing cost. Then attack coefficient of each node is calculating by considering the value of travelling cost and thus based upon this maximum attack coefficient value that node is captured by the adversary and thus the same procedure is followed until the whole network gets compromises.

There is a slight difference between DNA and DNPA. In DNA, the nodes belonging to dominating set are identified. After obtaining the nodes of dominating set, we calculate their path compromise ratio. After calculating path compromise ratio, we compute attack coefficient using capturing cost. Node with highest value of attack coefficient is selected in each round as a candidate node.
In DNPA, the nodes belonging to dominating sets are identified. After that node with maximum path compromise value and least capturing cost is identified as candidate node. We keep same list of dominating set and selects the nodes in each round with maximum PCR value with least capturing cost. We analyze the complexity in executing the following attack models. In BA, the nodes are captured blindly; thus, every situation is free from one another, making its complexity O(1).

In DNA, attacker determines a set of dominating nodes that connect the whole network. The path compromise ratio of these dominating nodes are used to select a node by adversary. Hence, the complexity becomes O (N3).

In DNPA, attacker determines a set of dominating nodes that connect the whole network. The path compromise ratio of these dominating nodes in the first round to select a node by adversary. Hence, the new complexity is O (N3).

MTA checks how various routes are compromised with attacking a link in every round. During the compromise of the path, it reduces its route compromise degree. After marking a node, it eliminates the compromised node with the route. Therefore, the complexity O(N2) [4].

In this new scheme, attacker firstly finds the dominating set of nodes in the network. The collection of dominating set of nodes are measured, and thus path compromise ratio of these nodes are calculated PCR gives the number of paths will be compromised by that node capturing. Thus the new complexity is O(N^3).

6. Case Study

This segment shows the unique effectiveness of the recommended system in determining the vulnerability of various links regarding that network. We produce considered an inactive network topology, as given by Figure 1. There are source node number 1 in the system and 1 sink node number 20, colored red in the network model. Different routes from the source node to the sink node are collected in P. The capturing cost of other nodes is taking random.

Fig 1 Network Topology
The study consist of a network of 20 nodes with node 1 as source and 20 as sink node represented red in colour. Fig 1 shows the network. In the first step dominating set of nodes are calculated. The set consist of 6 nodes, Node \{4,8,9,13,16,18\} represented green in colour and other nodes are represented by grey in colour.

\[ \text{PCR for node number 4} = \frac{11}{25}, \text{PCR for node number 8} = \frac{10}{25}, \text{PCR for node number 9} = \frac{6}{25}, \text{PCR for node number 13} = \frac{10}{25}, \text{PCR for node number 16} = \frac{7}{25}, \text{PCR for node number 18} = \frac{10}{25} \]

Fig. 2 Network Topology with dominating set nodes

Fig. 3 Network after compromise dominating nodes nodes
Figure 4 shows the path compromise ratio of different attack models namely DNA, BA, MTA, DNPA and DNTA. We observe that DNTA approaches to one when three nodes are captured whereas DNA approaches to one where four nodes are captured whereas MTA approaches to one when 5 nodes are captured. DNPA approaches to one when number of captured nodes are six and BA perform the worst in all five attack models. In BA, the nodes are captured randomly thus, number of routing paths compromised by candidate nodes in each round becomes least. Hence require large number of nodes to be captured by adversary to completely destroy the routing paths between source and sink node. In DNPA, the nodes belonging to dominating set are initially identified. After that the node with maximum PCR and least CC is selected. It destroys the network in five attacking rounds. In MTA, attacker aims to select the nodes carrying maximum traffic, thus nodes may or may not be part of routing path and hence require lesser number of nodes. In DNTA the node is captured with including the travelling cost to the node. In this network model with our case study gives best result for destroying the network by capturing least number of nodes. In DNA, it computes the dominating set nodes in each round and hence better effectiveness in destroying the routing paths. Thus, we observe that DNTA destroys the complete network with least number of attacking rounds and hence, has better performance among other attack models.

Fig 5 Number of attacking rounds Vs node capturing cost.
Fig. 5 depicts the relationship of number of attacking rounds Vs node captured cost. We observe that BA has maximum value of node capturing cost. It is due to the fact that this attack model does not consider any factor to destroy the network. It randomly selects the nodes of network and terminates when all routing paths are destroyed, hence generally have larger node capturing cost. In DNPA, the dominating set nodes are identified and this model terminates when all routing paths are destroyed. It also consider capturing cost of nodes. As dominating set of nodes are not selected in each round, thus, may result in larger number of captured nodes to destroy given set of routing paths and hence, larger value of node capturing cost. In MTA, it does not consider the routing paths concept and hence, results in larger number of rounds. In DNA, each attacking round recompute the dominating set of nodes and thus have greater effect on compromising the routing paths. It results in lesser value of node capturing cost with less number of captured nodes. In DNTA, travelling cost is also added, thus each round take care of travelling cost from previous location to current location. Thus has least number of captured nodes and hence least value of node capturing cost.

Fig 6  Number of attacking rounds Vs node travelling cost.

In BA, nodes are captured and are independent of previous location of capturing. Even, MTA, DNPA and DNA do not consider the travelling cost of a adversary in going from one location of capturing to other location of capturing. In DNTA, we consider the travelling cost and hence, it has least value as compare to others.

Fig 7 Number of attacking rounds Vs total energy cost
Figure 7 depicts the energy cost associated with different attacks. It is total energy cost including node capturing cost and traveling cost in destroying the complete network. It linearly depends on number of captured nodes. AS MTA and BA does not consider the capturing cost. Thus has high energy cost. In DNPA, the number of captured nodes is greater than MTA. Hence, has larger energy cost than MTA. As DNA and DNTA gives better result in capturing the minimum number of nodes to compromise the network and thus has least energy cost. Thus, total energy cost associated with DNTA is minimum.

7. Conclusion and future scope

Node capturing is one of the most prominent attack that destroys the integrity and security of network. The proposed work presents three improved attack models namely DNA, DNPA and DNTA. These attack models uses dominating set nodes, path compromise ratio, capturing cost and travelling cost in assessing the risk of adversarial attack during node capture. The proposed models are evaluated in terms of attacking rounds, capturing cost, travelling cost, total energy cost. It is found that DNTA out performs the other in all three performance metrics. Finally an application is also given on how to use the attack coefficient of nodes in deciding how many times hash functions is applied on redistributed keys. It makes the hash scheme more realistic by reducing unnecessary hash computations and hence, lowers the overall computation complexity. In future, we work on further enhancing of proposed attack models with more vulnerability factors of the network.

8. References

[1] Lin, C., Wu, G., Qiu, T., & Deng, J. (2016). A low-capturing cost node capture attack algorithm for wireless sensor networks. International Journal of Communication Systems, 29(7), 1251-1268.
[2] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: a survey. Computer networks, 38(4), 393-422.
[3] Du, W., Deng, J., Han, Y. S., Chen, S., & Varshney, P. K. (2004, March). A key management scheme for wireless sensor networks using deployment knowledge. In IEEE INFOCOM 2004 (Vol. 1). IEEE.
[4] Ahlawat, P., & Dave, M. (2018). A capturing cost-effective attack matrix based key management scheme with dominance key set for wireless sensor network security. International Journal of Communication Systems, 31(12), e3713.
[5] Ahlawat, P., & Dave, M. (2017). A hybrid approach for path vulnerability matrix on random key predistribution for wireless sensor networks. Wireless Personal Communications, 94(4), 3327-3353.
[6] Du, D. Z., Thai, M. T., Li, Y., Liu, D., & Zhu, S. (2006, January). Strongly connected dominating sets in wireless sensor networks with unidirectional links. In Asia-Pacific Web Conference (pp. 13-24). Springer, Berlin, Heidelberg.
[7] Tague, P., & Poovendran, R. (2008, September). Modeling node capture attacks in wireless sensor networks. In 2008 46th Annual Allerton Conference on Communication, Control, and Computing (pp. 1221-1224). IEEE.
[8] Mohanty, J. P., Mandal, C., Reade, C., & Das, A. (2016). Construction of minimum connected dominating set in wireless sensor networks using pseudo dominating set. Ad Hoc Networks, 42, 61-73.
[9] Lin, C., Qiu, T., Obaidat, M. S., Yu, C. W., Yao, L., & Wu, G. (2016). MREA: a minimum
resource expenditure node capture attack in wireless sensor networks. Security and Communication Networks, 9(18), 5502-5517.

[10] Lin, C., & Wu, G. (2013). Enhancing the attacking efficiency of the node capture attack in WSN: a matrix approach. The Journal of Supercomputing, 66(2), 989-1007.

[11] Lin, C., Wu, G., Yu, C. W., & Yao, L. (2015). Maximizing destructiveness of node capture attack in wireless sensor networks. The Journal of Supercomputing, 71(8), 3181-3212.

[12] Bonaci, T., Bushnell, L., & Poovendran, R. (2010, December). Node capture attacks in wireless sensor networks: A system theoretic approach. In 49th IEEE Conference on Decision and Control (CDC) (pp. 6765-6772). IEEE.

[13] Mishra, A. K., & Turuk, A. K. (2011, February). Adversary information gathering model for node capture attack in wireless sensor networks. In 2011 international conference on devices and communications (ICDeCom) (pp. 1-5). IEEE.

[14] Lin, C., Wu, G., Yim, K., Yao, L., & Hou, G. (2015, July). Compromising ad-hoc networks by attacking weakly connected dominating set. In 2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (pp. 213-220). IEEE.

[15] Bharathi, M. V., Tanguturi, R. C., Jayakumar, C., & Selvamani, K. (2012, December). Node capture attack in Wireless Sensor Network: A survey. In 2012 IEEE International Conference on Computational Intelligence and Computing Research (pp. 1-3). IEEE.

[16] Yang, Z., Li, P., Bao, Y., & Huang, X. (2019, December). A Multi-Dominating-Subtree-based Minimum Connected Dominating Set Construction Algorithm. In 2019 IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC) (Vol. 1, pp. 1077-1082). IEEE.

[17] Qin, R., Sun, Q., You, X., & Yuan, X. (2012, January). A key management scheme for manually deployed wireless sensor networks based on dual directional hash chains. In 2012 Second International Conference on Intelligent System Design and Engineering Application (pp. 752-755). IEEE.