Perform Active & DDoS Attack in Data Sharing Schemes using Network

Prof. Shailesh Hule,Nisha Biradar, Dhanashree Chavan,Girish Gaikwad,Siddharth Bhavsar
Pimpri Chinchwad College Of Engineering

Abstract: Wireless networks area unit progressively being deployed in security-critical applications. thanks to their inherent resource-constrained characteristics, they're susceptible to totally different security attacks may be a variety of attack that seriously affects information assortment. To tackle that challenge, a vigorous detection-based security and trust routing theme named trust is projected for wireless networks. the foremost vital innovation of trust is that it avoids attack through the active creation of variety of notice on routes to quickly detect and acquire nodal trust and therefore will increase the information route security. additional significantly, the generation and distribution of detection routes area unit given within the trust theme, which might totally use to realize the specified security and energy potency. Theoretical analysis and results indicate that the performance of the trust theme is healthier than that of previous studies. trust will considerably improve the information route success chance, ability against attacks and might optimize network life.

I INTRODUCTION:

Wireless Networks square measure rising as a promising technology due to their wide selection of applications in industrial, environmental observance, military and civilian domains. because of economic concerns, the nodes square measure typically easy and low price. they're usually unattended, however, and square measure thence seemingly to suffer from differing types of attacks. Aactive attack is one amongst the foremost typical attacks. The mortal compromises a node and drops all packets that square measure routed via this node, leading to sensitive knowledge being discarded or unable to be forwarded to the sink. as a result of the network makes choices looking on the nodes perceived knowledge, the result is that the network can fully fail and, create incorrect choices. Therefore, a way to discover and avoid active attack is of nice significance for security in wireless network.

Wireless Networks are rising as a promising technology thanks to their wide selection of applications in industrial, environmental watching, military and civilian domains. because of economic concerns, the nodes far sometimes straightforward and low value. they're usually unattended, however, and ar thus probably to suffer from differing kinds of attacks. Aactive attack is one in every of the foremost typical attacks. The someone compromises a node and drops all packets that are routed via this node, leading to sensitive information being discarded or unable to be forwarded to the sink.

II LITERATURE SURVEY

1.Paper Name: An Inter-domain Collaboration Scheme to Remedy DDoS Attacks in Computer Networks.

Authors: Steven Simpson, Syed Noorul hassan Shirazi, Angelos Marnerides Member, Dimitrios Pezaros Senior Member, IEEE, David Hutchison

Description: Distributed Denial-of-Service (DDoS) attacks continue to trouble network operators and service providers, and with increasing intensity. Effective response to DDoS can be slow (because of manual diagnosis and interaction) and potentially self-defeating (as indiscriminate filtering accomplishes a likely goal of the attacker), and this is the result of the discrepancy between the service provider's flow-based, application-level view of traffic and the network operator's packet-based, network-level view and limited functionality.

2. Paper Name: Mobile Target Detection in Wireless Sensor Networks With Adjustable Sensing Frequency.

Authors: Yanling Hu, Mianxiong Dong, Member, IEEE, Kaoru Ota, Member, IEEE, Anfeng Liu, and MinyiGuo, Senior Member, IEEE

Description: How to sense and monitor the environment with high quality is an important research subject in the Internet of Things (IOT). This paper deals with the important issue of the balance between the quality of target detection and lifetime in wireless sensor networks. Two target-monitoring schemes are proposed. One scheme is Target Detection with Sensing Frequency K(TDSFK), which distributes the sensing time that currently is only on a portion of the sensing period into the entire sensing period. That is, the sensing frequency increases from 1 to K.

3. Paper Name: Joint Optimization of Lifetime and Transport Delay under Reliability Constraint Wireless Sensor Networks[3].

Author: Mianxiong Dong, Member IEEE, Kaoru Ota, Member IEEE, Anfeng Liu and MinyiGuo, Senior Member, IEEE

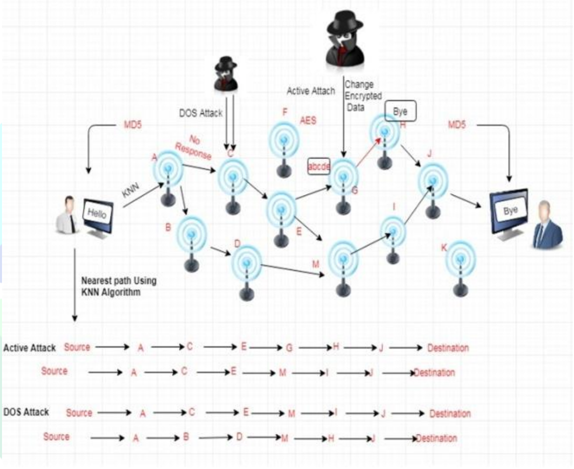
Description: This paper first presents an analysis strategy to meet requirements of a sensing application through trade-offs between the energy consumption(lifetime) and source-to-sink transport delay under reliability constraint wireless sensor networks. A novel data gathering protocol named Broadcasting Combined with Multi-NACK/ACK (BCMN/A) protocol is proposed based on the analysis strategy [2]. The BCMN/A protocol achieves energy and delay efficiency during the data gathering process both in intra-cluster and inter cluster.

4. Paper Name: Energy Provisionimng in Wireless Rechargeable Sensor Networks.

Author: Mohammad Mannan and P.C. van Oorschot

Description: Wireless rechargeable sensor networks (WRSNs) have emerged as an alternative to solving the challenges of size and operation time posed by traditional battery-powered systems. In this paper, author study a WRSN built from the industrial wireless identification and sensing platform (WISP)and commercial of the-shelf RFID readers. The paper-thin WISP tags serve as sensors and can harvest energy from RF signals transmitted by the readers.

III SYSTEM ARCHITECTURE:


DOS Attack
Active Attach
Change Encrypted Data
Bye
MD5
MD5
AES
No Response
abcde
KNN
Hello
Bye
A
B
C
D
E
F
G
H
I
J
K
M
Nearest path Using KNN Algorithm
Active Attack Source → A → C → E → G → H → J → Destination
Source → A → C → E → M → I → J → Destination
DOS Attack Source → A → C → E → M → I → J → Destination
Source → A → B → D → M → H → J → Destination

IV MATHEMATICAL MODEL

Let S is the Whole System Consists:

S= { V, E, P, G }.

Where,

1. V is the set of all the network nodes.

2. E is the set of all the links between the nodes in the network.

3. P is path function which defines the path between the two nodes.

4. Let G is a graph.

Suppose, G (V, E) from each path, the node u, which generates the packet and the original destination v. Where u and v are two nodes in the network .i.e. u V and v V of the attacked packet can be got.We denote the location of the attacker, i.e., the nearest router or the origin by s,

Where, s ∈ V.

Procedure:

1. For each path backscatter message, at first we check whether it belongs to the classes i.e. dataset or source list. If yes, the reflector should be near the attacker.

2. We simply use the source AS of the message as the location of the attacker. If the message does not belong to the types, it is mapped into an AS tuple.

3. We determine whether the AS tuple can accurately locate the source AS of the attacker based on our proposed mechanisms. Then if the AS tuple can accurately locate the source AS of the message, the source AS of the spoofer is just this AS.

4. Then we also use the source AS as the location of the spoofer.

V ALGORITHM DETAILS

Dijkstra's Algorithm

1. It maintains a list of unvisited vertices.
2. It chooses a vertex (the source) and assigns a maximum possible cost (i.e. infinity) to every other vertex.
3. The cost of the source remains zero as it actually takes nothing to reach from the source vertex to itself.
4. In every subsequent step of the algorithm it tries to improve(minimize) the cost for each vertex. Here the cost can be distance, money or time taken to reach that vertex from the source vertex. The minimization of cost is a multi-step process.
    1. For each unvisited neighbor (vertex 2, vertex 3, vertex 4) of the current vertex (vertex 1) calculate the new cost from the vertex (vertex 1).
    2. For e.g. the new cost of vertex 2 is calculated as the minimum of the two ((existing cost of vertex 2) or (sum of cost of vertex 1 + the cost of edge from vertex 1 to vertex 2))
5. When all the neighbors of the current node are considered, it marks the current node as visited and is removed from the unvisited list.
6. Select a vertex from the list of unvisited nodes (which has the smallest cost) and repeat step 4.
7. At the end there will be no possibilities to improve it further and then the algorithm ends

AES Algorithms Steps

1. Derive the set of round keys from the cipher key.

2. Initialize the state array with the block data (plaintext).

3. Add the initial round key to the starting state array.

4. Perform nine rounds of state manipulation.

5. Perform the tenth and final round of state manipulation.

6. Copy the final state array out as the encrypted data (ciphertext).

MD5 Algoruthm:

Step 1. Append Padding Bits

Step 2. Append Length

Step 3. Initialize MD Buffer

Step 4. Process Message in 16-Word Blocks

Step 5. Output

CONCLUSION

In the results of this analysis, we have a tendency to developed the trust analysis methodology that enables estimating the values of node work and remaining power. The estimation of those parameters with threshold analysis, once we calculate the chance for values to suit the arrogance interval, permits police investigation malicious options of individual nodes. we have a tendency to additionally estimate initial and second order errors. the brink of occurring errors with the quantity of malicious nodes but seventieth permits to observe and to dam malicious nodes with quite high potency. With the quantity of malicious nodes larger than seventieth, the exactness diminishes, but within the case of thousand nodes, that square measure settled in giant areas, it's extraordinarily arduous for a possible interloper to exceed even five hundredth threshold of malicious nodes. The environmental restrictions of BP cloth build it appropriate for hardware acceleration (e.g., with NetFPGA), demonstrating the practicability of preparation of Antidose in ASes with superior and low-programmability instrumentality. The techniques and principles used by Antidose cut back the barriers to AS operators managing the automated mitigation of bandwidth-saturating DDoS attacks. sensible and sturdy proof-delivery/white listing mechanisms stay open problems.

REFERNCES:

1] Yuxin Liu, Mianxiong Dong, Member, IEEE, Kaoru Ota, Member, IEEE,Anfeng Liu ”Active Trust Secure and trustable routing in wireless sensor network”IEEE System Journal, Doi: 10.1109/JSYST.2014.2308391, 2016.

[2] Y. Hu, M. Dong, K. Ota, et al.” Mobile Target Detection in Wireless SensorNetworks with Adjustable Sensing Frequency,” IEEE System Journal, Doi:10.1109/JSYST.2014.2308391, 2014.

[3] M. Dong, K. Ota, A. Liu, et al. ” Joint Optimization of Lifetime and TransportDelay under Reliability Constraint Wireless Sensor Networks”, IEEETransactions on Parallel and Distributed Systems, vol. 27, no. 1, pp. 225-236, 2016.

[4] S. He, J. Chen, F. Jiang, et al. ” Energy provisioning in wireless rechargeable sensor networks”, IEEE transactions on mobile computing, vol. 12, no.10, pp. 1931-1942, 2013.

[5] X. Liu, M. Dong, K. Ota, P. Hung, A. Liu. ”Service Pricing Decision in Cyber-Physical Systems: Insights from Game Theory”, IEEE Transactions on Services Computing, vol. 9, no. 2, pp. 186-198, 2016

[6] C. Zhu, H. Nicanfar, V. C. M. Leung, et al. ”An Authenticated Trust andReputation Calculation and Management System for Cloud and Sensor NetworksIntegration”, IEEE Transactions on Information Forensics and Security,vol. 10, no. 1, pp. 118-131, 2015.

[7] Y. Zhang, S. He, J. Chen. ” Data Gathering Optimization by DynamicSensing and Routing in Rechargeable Sensor Networks”, IEEE/ACM Transactionson network, doi:10.1109/TNET.2015.2425146, 2015.

[8] H. C. Leligou, P. Trakadas, S. Maniatis, P. Karkazis, T. Zahariadis, ” Combiningtrust with location information for routing in wireless sensor networks,”Wireless Communications and Mobile Computing , vol. 12, no. 12, pp. 1091-1103, 2012.

[9] Y. L. Yu, K. Q. Li, W. L. Zhou, P. Li, ” Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures”, Journal of Network and Computer Applications, vol. 35, no. 3, pp. 867-880, 2012.

[10] C. Karlof, U. Shankar, J.D. Tygar, and D. Wagner, ” Dynamic Pharming Attacks and Locked Same-Origin Policies”, Proc. 14th ACM Conf. Computer and Comm. Security (CCS), pp. 58-71, 2007.