Content Sharing and Trustworthiness Routing In Networks

Nisha Biradar, Dhanashree Chavan, Girish Gaikwad, Siddharth Bhavsar, Prof. Shailesh Hule
DEPARTMENT OF COMPUTER ENGINEERING, PCET's PIMPRI CHINCHWAD COLLEGE OF ENGINEERING

Abstract:

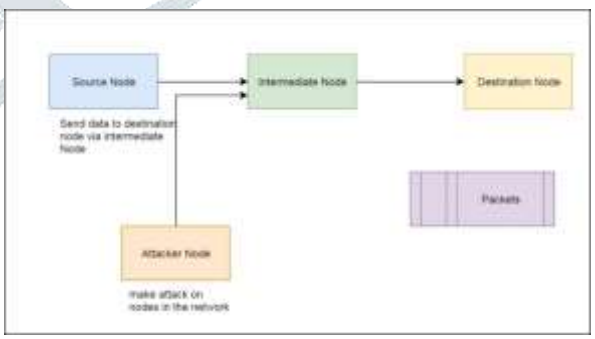
Wireless sensor networks (WSNs) are increasingly being deployed in security-critical applications. Because of their inherent resource-constrained characteristics, they are prone to different security attacks, and a black hole attack is a type of attack that seriously affects data collection. To tackle that challenge, an active detection-based security and trust routing scheme named Active Trust is proposed for WSNs. The most important innovation of Active Trust is that it avoids black holes through the active creation of a number of detection routes to quickly detect and obtain nodal trust and thus increases the data route security. More importantly, the generation and distribution of detection routes are given in the Active Trust scheme, which can fully use to achieve the desired security and energy efficiency. Theoretical analysis and results indicate that the performance of the Active Trust scheme is better than that of previous studies. Active Trust can significantly improve the data route success probability, ability against black hole attacks and can optimize network lifetime.

***Keywords*:** Security, Wireless Sensor Network, Trustable Routing, Networking.

1. Introduction:

Wireless Sensor Networks (WSNs) are emerging as a promising technology because of their wide range of applications in industrial, environmental monitoring, military and civilian domains. Due to economic considerations, the nodes are usually simple and low cost. They are often unattended, however, and are hence likely to suffer from different types of attacks. A black hole attack (BLA) is one of the most typical attacks. The adversary compromises a node and drops all packets that are routed via this node, resulting in sensitive data being discarded or unable to be forwarded to the sink. Because the network makes decisions depending on the nodes sensed data, the effect is that the network will completely fail and, make incorrect decisions. Therefore, how to detect and avoid BLA is of great significance for security in WSNs.

2. Architecture Diagram



3. Literature Survey:

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

Authors: Steven Simpson, Syed NoorulhassanShirazi, AngelosMarnerides Member, DimitriosPezaros Senior Member, IEEE, David Hutchison

Description: Distributed Denial-of-Service (DDoS) attacks con-tinue 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 inWireless Sensor NetworksWith 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 Provisioning 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.

4. Mathematical Modeling

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.

5. Algorithm:

1.KNN Algorithm

Step 1: Using KNN –K Nearest Neighbour Algorithm search the nearest node based on default location.
Step 2: Nearest node status check if node is hack ignore the select nearest node.
Step 3: Again search the another nearest node ignore 1st nearest.
Step 4: Nearest node is ok means not attack from Attacker.
Step 5: Verify the nearest node is final destination node.
Step 6: If nearest node is final destination node, then stop
the searching nearest node.

2.AES Algorithm

Step 1: Read data from Buffered Data Class and send as a input to cipher class for convert data in encryption.
Step 2: Generate the Public key for Encrypt data.
Step 3: call the init method of cipher class implement by java, & pass the plain text, public key.
Step 4: result data is encrypted.Also AES algorithm is used for decrypt data using secret or private key.

3.MD5 Algorithm

Step 1: Generated the digest value on data send from source to destination node.
Step 2: Verify the digest value at the time of send data source to destination.
Step 3: verification response to Source node if data is Hack or Change from another node.

5. Conclusion:

We have presented Antidose, a scheme allowing participating ASes to mitigate the effects of a Distributed Denialof-Service attack on a target, and which is able to control whitelists within ASes upstream of the saturation zone of the attack. Effectively, through interaction with only immediate neighbors, an AS with only a low-level network view of traffic is given the ability to discriminate legitimate packets from likely attack packets using criteria set by the target, which has a higher-level (transport or application) view. We have presented an implementation of Antidose's critical component, the verification filter (VF), and analyzed its behavior in the face of various counter-attacks. The Antidose VF is sufficiently omputationally simple to be deployed in BPFabric, a restricted execution environment for switching fabric, with the eavy-weight operations of hashing and signature verification handled

externally and therefore potentially in hardware. We demonstrated that, even in this restricted environment, the VF correctly discriminates traffic according to the target's ever-developing definition of legitimate and malicious peers, and that Bloom ilters are effective as whitelists even when there are thousands of simultaneous or recent legitimate clients.

6. References:

[1] 1. Abramov E.S., Basan E.S. Development of a model of aprotected cluster wireless sensor network. / News of SFedU.Technical science./ □ 12 (149) 2013 Thematic issue Informationsecurity. Publishing house TIT SFedU in Taganrog . – P.48-56.

[2] 2. Basan E.S., Makarevich O.B., Abramov E.S. Development of asystem for detecting attacks for a cluster wireless sensor network /Information Counteraction to Terrorism Threats / □20. 2013.TITU Publishing House in Taganrog – P. 134-140

[3] 3. K Govindan, P Mohapatra. Trust computations and trustdynamics in mobile ad hoc networks: A survey IEEECommunications Surveys & Tutorials 14 (2), 279-298.

[4] 4. Abramov E.S., Basan E.S. Analysis of scenarios of attacks onwireless sensor networks / Materials of the XIII InternationalScientific and Practical Conference "IB–2013" / Part 1. – Taganrog: Publishing house of TIT SFedU, 2012. –P.60-65.

[5] 5. Shelukhin O.I., Simonyan A.G., IvanovYu.A. Features ofDDoS attacks in wireless networks // T–Comm –Telecommunications and Transport No.11/2012. p.67-71.

[6] 6. Belfer R.A., Ogurtsov I.C. Protection of information security ofsensor network of cluster architecture using the intrusion detectionmechanism // Bulletin of MSTU. N.E. Bauman: an electronicpublication. 2013. pp. 1-7.

[7] 7. DipaliWirmani, ManasHemrajani, ShringaritsaChandel. Anexponential confidence mechanism for detecting the attack ofblack holes in a wireless sensor network.International Journal ofSoft Computing and Design (IJSCE). 2014. pp. 14-16

[8] 8. Grishechkina T.A. Analysis of attacks on network protocols inmobile sensor networks ad hoc. Izvestiya of Southern FederalUniversity. Engineering Sciences, Issue.No.12(137).2012.p.68-74.

[9] 9. Basan A.S., Basan E.S., Makarevich □.B. Methodology ofcounteracting the attacks of wireless sensor networks based on theinternational conference Trust. 2016 on cybernetic distributedcomputing and knowledge discovery.P.409-4012.

[10] 10. Basan A.S., Basan E.S., Makarevich □.B. Development of ahierarchical trust management system for a wireless sensornetwork based on a mobile cluster.Continuation of SIN '16Proceedings of the IX International Conference on Security ofInformation and Networks, 2016, P.116-122.