ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

Exploiting Channel-Aware Reputation System for Packet Drop Attack Detection in Wireless Ad-hoc Network

Ashwini Prakash More[1], Prof. Deepak Gupta [2]

P.G. Student, Department of Computer Engineering, Sidhhant College of Engineering, Sudumbare, Pune Maharashtra, India[1]

Associate Professor, Department of Computer Engineering, Sidhhant College of Engineering, Sudumbare, Pune Maharashtra, India[2]

ABSTRACT: Wireless networks square measure utilized in numerous areas, like battlefields, traffic police investigation, healthcare, and environmental observation. Wireless networks square measure susceptible to selective forwarding attacks which can maliciously drop a group of forwarding packets to degrade network performance and jeopardize the data integrity. Projected a Channel-aware name System with adaptive threshold (CRS-A) to detect selective forwarding attacks in wireless network by exploitation bloom filter. The CRS-A evaluates the data forwarding behaviors of device nodes, in step with the deviation of the monitored packet loss and thus the derived ancient loss. To optimize the detection accuracy of CRS-A, system derives the simplest threshold for forwarding analysis that's adaptive to the time varied channel condition and thus the derived attack possibilities of compromised nodes or traditional. It poses a wonderful challenge to differentiate the malicious drop and ancient packet loss by exploitation bloom filter algorithmic program.

KEYWORDS: Wireless Ad-hoc Network, Selective Forwarding Attack, Packet Dropping, Bloom Filter

I. INTRODUCTION

Wireless ad-hoc networks contain completely different nodes. These nodes communicate with a huge vary of very little nodes via radio links. The selective forwarding attacks area unit hid by the normal packet losses, complicating the attack detection mistreatment bloom filter. Therefore, it's tough to search out the selective forwarding attacks and improve the network performance. Most of connected works specialise in observation the packet losses in each transmission link and analytic the nodes with high packet loss rates from the data forwarding path. These solutions can improve the data delivery magnitude relation or network turnout but have little or no impact on detection selective forwarding attacks. Since the foremost challenge of attack detection is to differentiate the malicious drop from ancient packet loss, the normal packet loss rate of the transmission link have to be compelled to be thought of inside the forwarding analysis.
Most of the prevailing studies on selective forwarding attacks specialise in attack detection assumptive that the wireless channels area unit error free.

1. It could also be a tricky task to differentiate between these losses and establish the forwarding attacks to spice up the network performance.
2. The ancient packet loss rate extravagantly depends on the wireless channel quality that varies spatially and temporally.
3. The system uses the concept of measured or enumerable ancient packet loss rate to search out selective forwarding attacks mistreatment bloom filter, then likelihood is that that there that the innocent nodes are going to be called attackers thanks to the time-varied channel condition.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

The system sight the packet dropping are going to be as a results of the grey-hole attacks i.e. by malicious nodes, ancient loss events like unhealthy channel or medium access collision. Designed a channel aware detection (CAD) algorithmic rule which can establish the selective forwarding attackers by filtering the normal channel losses. The CAD follows a pair of procedures, traffic observation and channel estimation. Channel estimation is regarding the estimation of ancient loss rate thanks to unhealthy channel quality or medium access collision. Traffic observation is to appear at the actual loss rate. Say if the monitored loss rate at positive hops exceeds the enumerable loss rate, then those nodes involved area unit called attackers.

The existing works into 2 categories: neighbour police investigation primarily theme and acknowledgement based. this relies on the various observation techniques for information forwarding.

1. Acknowledgment based Defence Techniques

In this variety of theme an acknowledgement is received from the nodes within the routing path to seek out the packet loss if any. during this theme the nodes square measure designated willy-nilly and thought of because the checkpoints to come back acknowledgements for every received packet. If something ascertained to be suspicious then an alarm packet is generated and sent to the supply node. During this theme an intrusion-detection system named increased adaptive acknowledgement (EAACK) for mobile adhoc network is used.

2. Neighbor-surveillance based Defense Techniques

This is hardware wherever the detector nodes will monitor the forwarding behaviours of their neighboringnodes and might record the packet loss precisely. Every node includes a table to record and maintain the performance of the neighbor nodes that is predicated on the forwarding observation of the neighboringnodes. The nodes with less name values area unit far away from the routing path. This works just for the monitored packet loss throughout the forwarding.

II. LITERATURE SURVEY

1. I. Butun, S. Morgera, and R. Sankar, [2] discuss the applications based on the Wireless Sensor Networks are growing very fast. The application areas include agriculture, healthcare, military, hospitality management, mobiles and many others. Stopping these attacks or enhancing the security of the WSN system various intrusion detection policies are developed till date to detect the nodes that are not working normally. Out of various detection techniques three major categories explored in this paper are Anomaly detection, Misuse detection and Specification- based detection. Here in this review paper various attacks on Wireless Sensor Networks and existing Intrusion detection techniques are discussed to detect the compromised node/s.

Advantages: Wireless Sensor Networks are growing very fast & IDS technique to detect the compromised node/s.

Limitation: Wireless sensor nodes do not have a large battery life, larger transmission range and more computational power. They have limited memory.

2. Y. Zou, X. Wang, and W. Shen, [3] in this paper they contemplate a psychological feature radio network that consists of 1 psychological feature base station (CBS) and multiple psychological feature users (CUs) within the presence of multiple eavesdroppers, wherever CUs transmit their information packets to CBS beneath a primary user's quality of service (QoS) constraint whereas the auditor decide to stop the psychological feature transmissions from CUs to CBS. Specifically, a psychological feature user (CU) that satisfies the first QoS demand and maximizes the possible secrecy rate of psychological feature transmissions is regular to transmit its information packet. For the comparison purpose, they conjointly examine the normal multiuser programing and also the artificial noise schemes.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

Advantages: Multiuser scheduling and the artificial noise approach as benchmark schemes.

Limitations: They have not considered user fairness in the multiuser scheduling for improving the cognitive radio security against eavesdropping attacks.

3. Y. Zhang, L. Lazos, and W. Kozma [4] they address the matter of characteristic and separate offend nodes that refuse to forward packets in multi-hop unplanned networks. we tend to develop a comprehensive system known as Audit-based wrongdoing Detection (AMD) that effectively and with efficiency isolates each continuous and selective packet droppers. The AMD system integrates name management, trustworthy route discovery, and identification of misbehaving nodes supported activity audits. Compared to previous strategies, AMD evaluates node behavior on a per-packet basis, while not using energy-expensive overhearing techniques or intensive assent schemes.
Advantages: Detecting and isolating misbehaving nodes.

Limitations: Problem of identifying and isolating misbehaving nodes that refuse to forward packets in multi-hop ad hoc-networks.

Limitations: As AMD acknowledgement is too tedious and ends in high load.

4. Tao Shu, Marwan Krunz, [6] in a multi-hop wireless ad hoc network, packet losses are attributed to harsh channel conditions and intentional packet discard by malicious nodes. In this paper, while observing a sequence of packet losses, we are interested in determining whether losses are due to link errors only, or due to the combined effect of link errors and malicious drop. We are specifically interested in insider's attacks, whereby a malicious node that is part of the route exploits its knowledge of the communication context to selectively drop a small number of packets that are critical to network performance. Because the packet dropping rate in this case is comparable to the channel error rate, conventional algorithms that are based on detecting the packet loss rate cannot achieve satisfactory detection accuracy. To improve the detection accuracy, we propose to accomplishment the correlations between lost packets.

Advantages: To improve the detection accuracy.

Limitations: In a multi-hop wireless ad hoc network, packet losses are attributed to harsh channel conditions and intentional packet discard by malicious nodes.

III. PROPOSED SYSTEM

The proposed system CRS-A, which helps in evaluating the forwarding behaviours of attacker nodes with the expertise of adaptive detection threshold. Associate degree using bloom filter algorithm best detection threshold to gauge the forwarding behaviours to optimize the detection accuracy of CRS-A. This best threshold is scheduled for each transmission link really probabilistic method.

CRS-A is collaborated having a distributed and attack tolerant knowledge forwarding theme so as to simulate the forwarding cooperation of compromised nodes or more the data delivery magnitude relation of the network. As opposed to treatment of compromised nodes in the information forwarding it considers them time varied channel condition and attack possibilities of neighbouring nodes in selecting forwarding nodes.

Advantages of Proposed System:

1. Efficient and reliable than existing systems.
2. Accurate detection of actual packet drops by malicious nodes and system packet drops by some feasible reasons like system failure due to capacity etc.
3. Increasing packet delivery ratio.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

4. Designed secure communication channel for secure communication between dynamic networks.

Application of Proposed System:

In military and civilian applications for confidetional communication.

IV. SYSTEM ARCHITECTURE

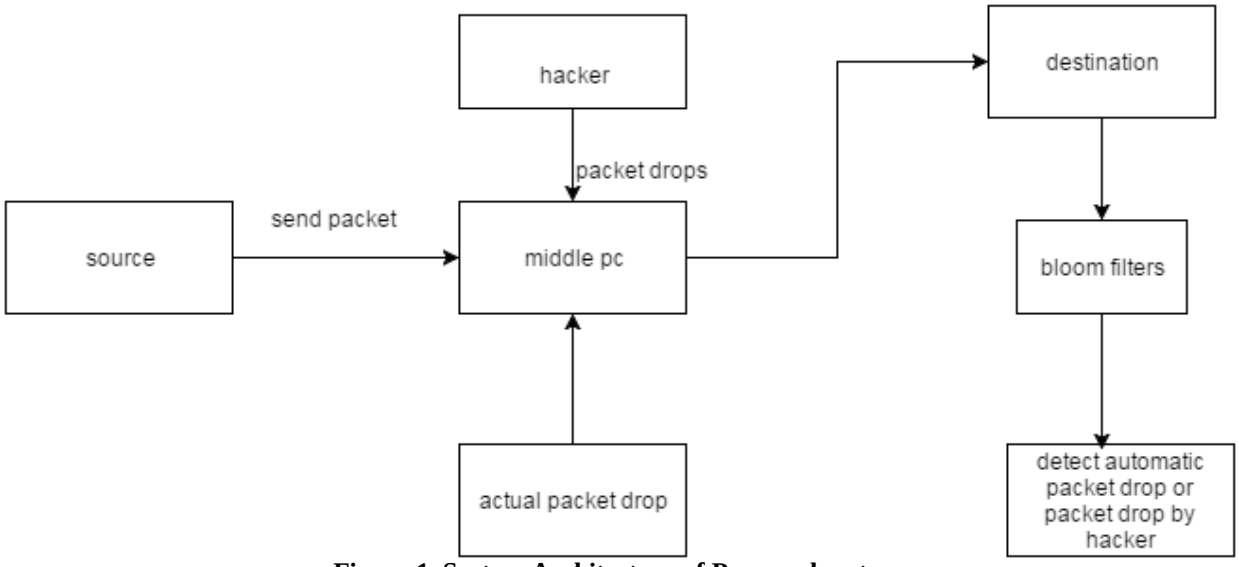

Figure 1. System Architecture of Proposed system

System Design and Implementation:

1st pc (source/sender):

The sender pc enter the destination IP address to send message this message is in the form of text file (the text file must contains at least 3 lines of text)

The sender will browses the file from system and sends to destination. At the back end the system will create 3 packages and divide the data which sender is sending to destination (i.e. total number of lines divided by 3 i.e. the data divided into 3 packages, encrypts them and sends to destination with secret key to decrypts and view data packets).

A unique sequence number will be attached to each packet while sending which is used at destination side to filter the packets.

2nd pc (mediator/intermediate/hacker):

This pc will acts as receiver i.e. it receives the packets from A on behalf of B and also acts as sender on behalf of A and will send packets to B.

1. Malicious packet drop:

The mediator system will acts like hacker who drops packets, changes destination address.

Assume A sender is sending data to B destination then, in between hacker C will drops or modifies or changes destination address i.e. to D.

When C alter the any one packet among 3 or all the packets that time the sequence number which was assigned initially it will automatically increases or updates.

On the basis of current sequence number the system will filter the malicious packets received.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

2. System packet drop:
In this packet drops are occurred due to systems incompatibility problem.
If the sender is sending the data of 10MB but the capacity of node is only 7MB then it will accept only 7MB data only drops remaining 3MB of data, so here packet drops are occurred due to system failure not because of malicious node.
Here the system keeps 3 buffers of size 10 MB, 7 MB and 5 MB. To show different packet drop rate.

3rd pc (destination/receiver):
This is the destination pc it will receive the packets from sender and send ack to sender after system gives the report of bloom filter about packet drop attack or destination IP change or also checks for provenance for data.

4th pc (destination1/receiver1):
This is also destination pc, comes into picture when hacker changes destination IP.
If suppose this pc will try to open the packets the system will automatically send that packets to original destination, that packet may malicious or actual packets, the verification is done at actual destination side.

V. MATHEMATICAL MODEL

Let W be the whole system which consists:
W= {IP, PRO, OP}
IP is the input of system.
IP= {BS, G, N, L, K, H, d, ID, V, E, S, BF}.
Where,

1. Let BS is the Base Station which collects data from network.

2. Let G is the graph , G(N,L)
   Where, N is the set of nodes.
   $N = \{ni|, 1 \leq i \leq |N|\}$ is the set of nodes,
   And L is the set of links, containing an element li,j for each pair of nodes ni and nj that are communicating directly with each other.
3. K is set of symmetric cryptographic key

4. H is a set of hash functions

   H = {h1, h2, ..., hk} .

5. E is edge setconsists of directed edges that connect sensor nodes.

6. d is the set of data packets,

Let G is acyclic graph G(V,E) where each vertex $v \in V$ is attributed to a specific node HOST(v) = n and represents the provenance record (i.e. nodeID) for that node.

Each vertex in the provenance graph is uniquely identified by a vertex ID (VID) which is generated by the host node using cryptographic hash functions.

Procedure:
Let S is a set of items
S = {s1, s2, ..., sn}
We use an array of m bits with k independent hash functions h1, h2, ..., hk.
The output of each hash function hi maps an item s uniformly to the range [0, m-1], i.e., an index in a m-bit array.
Let BF is the Bloom Filer, can be represented as {b0, . . . , bm−1}.
Initially all m bits are set to 0.
To insert an element $s \in S$ into a BF, s is hashed with all the k hash functions producing the values hi(s) ($1 \leq i \leq k$).
The bits corresponding to these values are then set to 1 in the bit array.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

To query the membership of an item s` within S, the bits at indices hi(s`) ($1 \leq i \leq k$) are checked. If any of them is 0, then certainly s` not within S. Otherwise, if all of the bits are set to 1, s`$\in$ S with high probability.

There exists a possibility of error which arises due to hashing collision that makes the elements in S collectively causing indices hi(s`) being set to 1 even if s` not within S. This is called a false positive.

V. RESULT ANALYSIS WITH GRAPH

Here, Whole System taken many more attribute for the input purpose but here author mainly focuses on the accuracy, time, storage and energy cost of system. Based on this attributes we getting following analytical result for our proposed system with respect to existing system.

	Existing	Proposed
A	4	10
B	5	10
C	8	3
D	5	8

Where,
A = Detection Accuracy.
B = Security.
C = Time.
D = Efficiency.

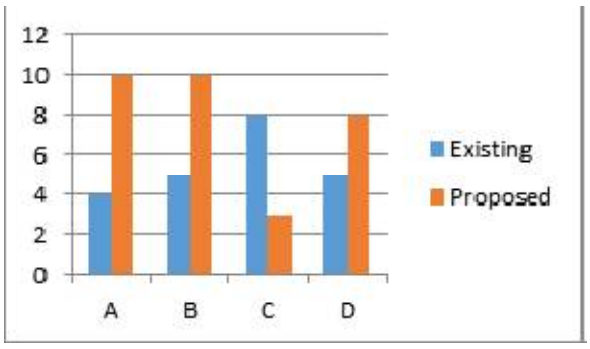

Figure 2. Existing System vs. Proposed System

VII. CONCLUSION

Within this project approach, we have got introduced a Channel Aware name System in corporate with adaptive detection threshold (CRS-A) in order to detect the selective forwarding attacks in WSNs using bloom filter algorithm. To differentiate between traditional packet loss and selective forwarding attacks, CRS-A uses the very thought of deviation relating to the calculable traditional packet loss and monitored packet loss. . All intermediate nodes are considered as internal eavesdroppers from which the confidential information needs to be protected. To provide confidentiality such setting, we propose encoding the material over long blocks of knowledge which can be transmitted over different paths.

REFERENCES

[1] J Ren, Y Zhang, K Zhang and X Shen, "Adaptive and Channel-Aware Detection of Selective Forwarding Attacks in Wireless Sensor Networks", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. XX, NO. XX, XXX 2016.
[2] I. Butun, S. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," IEEE Commun. Surv. & Tutor., vol. 16, no. 1, pp. 266–282, 2014.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

[3] Y. Zou, X. Wang, and W. Shen, "Physical-layer security with multiuser scheduling in cognitive radio networks," IEEE Trans. Commun., vol. 61, no. 12, pp. 5103–5113, 2013.
[4] Y. Zhang, L. Lazos, and W. Kozma, "Amd: Audit-based misbehavior detection in wireless ad hoc networks," IEEE Trans. Mob. Comput., prePrints, published online in Sept. 2013.
[5] X. Liang, X. Lin, and X. Shen, "Enabling trustworthy service evaluation in service-oriented mobile social networks," IEEE Trans. Parallel Distr. Sys., vol. 25, no. 2, pp. 310–320, 2014.
[6] J. Ren, Y. Zhang, K. Zhang, and X. Shen, "Exploiting channel-aware reputation system against selective forwarding attacks in wsns," in Proc. IEEE GLOBECOM, 2014, pp. 330–335.