A Novel Approach for Detecting Wormhole Attacks Using Expected Transmission Count Technique

Vartika Sharma [1], Anandhi G[2]
[1, 2]Department of Computer Engineering
[1,2] Assistant Professor, GSSSIETW,Mysuru

Abstract- *Wireless Sensor Networks are emerging as a promising platform for a variety of application areas. However many security issues impede its wide deployment in practice. The nature of the wireless communication, the fast deployment practices, and the hostile environments where they may be deployed, make them vulnerable to a wide range of security attacks. Among these attacks wormhole attack plays a major role. This paper analyzes and finds solution for wormhole attack and enhances the detection of innovative packets which is possibly done by DAWN. We rigorously prove that DAWN guarantees a good bound of successful detection rate. We perform analysis on the resistance of DAWN against collusion attacks. DAWN does not rely on any location information, global synchronization assumptions or special hardware/middleware. It is only based on the local information that can be obtained from regular network coding protocols, and thus the overhead of our algorithms is tolerable. The experimental results have verified the effectiveness and the efficiency of DAWN.*

Keywords- Wormhole, DAWN, Wireless Sensor Network, ETX

I. INTRODUCTION

The Wireless Sensor Network (WSN) is an emerging technology and has great potential to be employed in critical situations like battlefield and commercial application such as building, traffic surveillance, habitat monitoring and smart homes and many more scenarios [8]. In order to improve the system performance of wireless networks, network coding has been shown to an effective and promising approach and it constitutes a fundamentally different approach compared to traditional networks, where intermediate nodes store and forward packet as the original. One of the major challenges wireless sensor face today is security [12]. While the deployment of sensor nodes in an unattended environment makes the network vulnerable to a variety of potential attacks, the inherent power and memory limitation of sensor nodes makes conventional security solution unfeasible. Wireless Sensor Network is vulnerable to security attacks due to the broadcast nature of the transmission medium. Furthermore, Wireless Sensor Networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected [18].

Basically attacks are classified as Active attacks and Passive attacks [21]. Passive attacks include monitoring and listening of the communication channels by unauthorized attackers. The attack against privacy is passive in nature. The unauthorized attackers monitors, listens to and modifies data stream in the communication channels are known as Active attacks.

We summarize the contributions of this paper as follows, Section II describes the analysis of related work done by the various researchers for defending against wormhole attack. Proposed methodology and designing is demonstrated in Section III associated with algorithm and theorems. Section IV showcases the simulation results to prove the capability of this work. Finally Section V concludes the paper followed by the references.

- WORMHOLE ATTACK

Wormhole attack is a type of active attacks. In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them to another location, and retransmits them into the network [9].

The wormhole attack is a kind of tunneling attack, which is very dangerous and damaging to defend against even though the routing information is confidential, authenticated or encrypted. The adversary doesn’t need to have knowledge about the routing protocol or compromise the sensor nodes. In wormhole attack, two malicious nodes are connected through a low latency link, namely wormhole link [21]. A low latency can be realized through a network cable, other kind of wired link technology or just a long range out of band wireless transmission. Once the wormhole link is established, the adversary eavesdrops on packets at one end of the link, tunnels them through the wormhole link and replays the packets at the other end of the link. This makes the sensor nodes around the two ends of the wormhole link seem like neighbor nodes as though they are multi-hops away from each other actually.

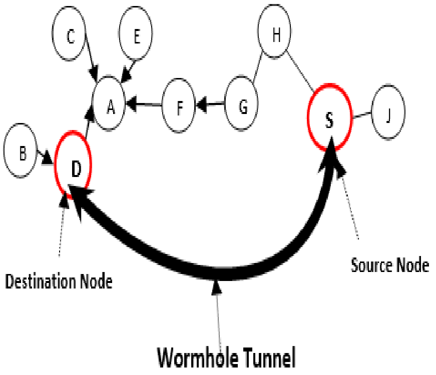

Fig 1: Example for Wormhole Attack

An example of wormhole attack is given in Figure 1.Node S and D are two malicious nodes placed by the adversary connected via a network cable. So node S and D are the two end points of the wormhole link. Node S receives packets, tunnels them through the wormhole link and replays the packets at node D and vice-versa [10]. As a result nodes in the neighborhood of node S will assume that all nodes in the neighborhood of node D are their neighbors and vice-versa.

By retransmitting the packets from the wormhole links, some victim node will have to process much more non-innovative packets that will waste their resources. The attackers can periodically turn on and off the wormhole links in data transmissions, confusing the system with fake link condition changes and making it unnecessarily return the routing process. To further quantify the impact of wormhole attacks in wireless network coding systems, we perform extensive experiments and investigate the results in Section 4.

- SECURITY GOALS

Sensor networks with limited processing power, storage, bandwidth, and energy require special security approaches [16][8]. The hardware and energy constraints of the sensors add difficulty to the security requirements of ad-hoc networks concerning availability, integrity, confidentiality, freshness, authentication, access control and non-repudiation [19].

II. RELATED WORK

Dr.G.Padmavathi, Mrs.D.Shanmugapriya [25] discusses a wide variety of attacks in wireless Sensor Networks and their classification mechanisms and different securities available to handle them including the challenges wireless Sensor Networks face today is security. While the deployment of sensor nodes in an unattended environment makes the networks vulnerable to a variety of potential attacks, the inherent power and memory limitations of sensor nodes makes conventional security solutions unfeasible.

This paper upheld the knowledge that sensor networks are inherently different from traditional wired networks as well as wireless important feature for the deployment of Wireless Sensor Networks.

Mohamed Lamine Messai[26] confronts proposing security solutions in WSN's because of their applications in both civilian and military domains. It also presents the challenges of security, classification of the different possible attacks in WSN's and the problems of security in each layer of the networks OSI model are discussed.

In the previous section, we have already discussed about the classification of attacks, that is, active and passive attacks. In this paper, the classification of attacks consists in distinguishing the passive attacks from the active attacks. The common known attack are Tampering, Black hole, Selective forwarding, Sybil attack, HELLO flood attack, Jamming, Blackmail attack, Exhaustion, Wormhole attack, Identity replication attack.

It also provides a layer based classification of defined attacks on the OSI model.

- Physical layer: Deals with the specification of the frequencies bands. This layer must ensure of the techniques of emissions, reception and modulation of data in a robust way. The attacks associated in the physical layer are very few, but at the same time, can be most difficult to prevent from Jamming on the same frequency that the network uses, and the physical attack of a node.

- Data Link Layer: This layer manages the access to the radio channel and control errors. The adversary can only induce collision in a one byte of a transmission to disturb the entire data packet.

- Network Layer: WSN's use communication multi-hops for routing the packets towards the destination. The attacks in this layer are: Black hole attack, Selective forwarding, Sybil attack, HELLO flood attack, Wormhole and Identity replication attack. The prevention of this kind of attacks invites to authenticate all messages.

Guowri Wu, Xiaojie Chen, Lin Yao, Youngjun Lee and Kangtsen Yin [27], Proposes a wormhole attack detection method based on the transmission range that exploits the local neighborhood information check without using extra hardware or clock synchronizations. Extensive simulations are conducted under different mobility models. Simulation results indicate that the proposed method can detect wormhole attacks effectively and efficiently in WSN's.

In this paper, through judging the nodes position, we can determine whether the node is in local network topology affected by the wormhole link. In the detection procedure, the neighborhood information of each node is updated and exchanged periodically between neighbors along the increment of the transmission range. A local topology that has a wormhole link finally reports a mismatch of the neighborhood information between nodes.

The simulation results also demonstrate that our wormhole detection method can achieve a high wormhole detection rate.

Yurong Xu,Guanling Chen,James Ford and Fillia Makedon [28] describes a distributed wormhole detection algorithm for wireless Sensor Networks, which detects wormholes based on the distortions they create in the network. Since wormhole attacks are passive in nature, the algorithms uses a hop counting technique as a probe procedure, reconstructs local maps in each node, and then uses a "diameter" feature to detect abnormalities caused by wormholes.

The wormhole geographic distributed detection (WGDD) algorithm also represents advancement over other wormhole detection algorithms because it does not require anchor nodes, additional hardware or the manual setup of network.

III. METHODOLOGY

In this section, we describe the technical specifications needed in this paper

3.1 EXPECTED TRANSMISSION COUNT

ETX has extensive applications in network coding systems [3],[4],[5],[12].In this paper, the ETX of a node u in the network coding system denotes the expected total number of transmission (including retransmission) that the source node should make, in order to make the node u receive one innovative packet successfully. A node of high ETX means it is difficult to make it heard from the source, usually because the node is far from the source and the links between them are very lossy. Thus, the metric of the network structure.

In existing works (e.g., [5],[17]), the ETXs are calculated based on the probabilities of packet loss between each pair of the nodes in the network. Let u and v be two nodes, and p (u ,v) be the probability of successful transmission between nodes u and v. For the simplest case, if the network only has a sender u and a recipient v, then the ETX of the sender u is 1.0, and the ETX of v is shown as equation (4):

$$ETX(v)=1/p\ (u, v).$$

The probability p (u, v) can be estimated based on the previous transmission record, using some statistical models like weighted means and window-based observation[5]. Based on (4), if the link between the nodes is very lossy, the ETX of v can be very high, indicating that it is difficult to deliver messages through the link loss probabilities. As we will talk about, the wormhole link connects two distant nodes with on reduces the ETXs significantly. The fact is heuristic to our algorithms.

Since our wormhole detection algorithm will rely on the values of ETXs, it is important to ensure that the system has appropriate defense against possible attacks on ETXs. In practice links loss probabilities used in ETXs calculation are measured and reported using small control packets sent among nodes and these packets are transmitted under conventional protocol instead of network coding. To protect these protocol from wormhole attacks, existing counter measures of wormhole in conventional wireless network can be leveraged such as [13], [15], [16]. To defend against other cheating and malicious behavior in measuring link loss probabilities, e.g., submitting untruthful reports, both cryptographic and incentive-mechanism approaches can be used [22].

3.2 THE DISTRIBUTED DETECTION ALGORITHM

We propose DAWN, a distributed algorithm to detect wormhole attacks in wireless network coding systems. We will perform rigorous analysis on the detection rate of our algorithm and its resistance against collusions.

3.2.1 ALGORITHM DESIGN

For any two nodes in the neighborhood, the one with lower ETX is supposed to receive novel packets earlier than the other one with high probabilities. In other words, innovative packets are transmitted from low ETX nodes to high ETX nodes with high probabilities. In order to monitor the innovative packets transmission direction, nodes will work collaboratively. In particular, DAWN has two phases on each node: 1) report packets direction observation results to its neighbors (Algorithm 1) *Detect* whether any attackers exist (Algorithm 2). The *Detect* phase is based on the received results from neighbors during the *Report* phase. Both of the algorithms are running on every node in the network. Algorithm 1 runs simultaneously while passing on the packets, and Algorithm 2 should be asynchronous for different nodes run at random time slots.

Algorithm 1: Report Function

Input: N(u): the set of *u*'s neighbors; the number of the novel packets u received from each neighbor in the last batch; δ:the threshold on ETX difference.

Output: S_V : the local observation results for each neighbor v ϵ N(u) ;Report message if any.

```
1: for v ϵ N(u) do
    2: denote $P_V$ the number of novel packet that u received from v during last batch
    3: if ETX (v)-ETX (u) δ and P v  > 0}then
        4: u broadcast the report r (u, v, 0);
        5: note: $r\ (u,\ v,\ 0)$ represents the report sent from $u$ about the suspicious wormhole behavior of $v$,with hop count 0.
        6: $S_v$ = 1;
    7: else
        8: $S_v$ =0;
    9: end if
10: end for
```

ort phase: As shown in algorithm 1, for each node, it will suspect that one neighbor is an attacker if it receives novel packets from the neighbor but the ETX of this neighbor is much higher than that of itself (i.e., the distance between the ETXs is greater than the threshold δ. It sends its judgment as a report to its neighbors (line 3-5). A node is called a judge node of a neighbor if the distance between their ETXs is greater than the threshold. Each report r is a tuple as equation (15):

$$r=(time,A_{suspect},A_{self},K_{pub},S_{novel},sig). \qquad (15)$$

Here, time is when the reporting node discovers the abnormal transmission. $A_{suspect}$ is the address of the suspected node, which sends out a novel packet and owns a higher ETX than the recipient's. A_{self} is the address of the reporting local node. Since any node can modify the report when forwarding it, we need to apply cryptographic techniques to protect the integrity of the reports. We use digital signatures of the report to defend against malicious modification, and abstract of the novel packet for administrative verification. Thus, we introduce symmetric cryptographic scheme into our system to make it more robust against attacks. In equation 15 Kpub is the public key of the reporting node.

S_{novel} is the set of the signatures of the received novel packets. Sig is the signature of the report. The signature are produced as Equation (16):

$$Sig=Encrypt\ (K_{sec},\ (Hash(p))). \qquad (16)$$

Here K_{sec} is the secre~~t~~ key of the reporting node. P is the novel packet that was received from the target.

Algorithm 2: The distributed detection algorithm for wormholes in wireless network coding systems (DAWN) on node u

Input: R: the set of reports received in the last batch; N(u):the set of u's neighbors; S_J: the local observation result of each neighbor j ϵ N(u); δ: the threshold.

Output: Detected wormhole attackers in N(u),if any.

```
1: for each report r(I, j, k) ϵ R do
    2: if ETX( j )-ETX( i ) ≤ $\delta\ OR\ i \in N(j) then$
        3: discard this report;
    4: else
        5: if j ∈ $N(u) then$
            6: $s_j \leftarrow s_j + 1$;
        7: end if
        8: if k<2 then
            9: forward this report r(I, j, k+1);
        10: end if
    11: end if
12: end for
13: for each $v$ ϵ $N(u)$ do
    14:let $C(v)$={i |i ϵ N(v) s.t. ETX (v)-ETX(i) δ
    15: if $S_v \geq \left\lceil \frac{|c(v)|+1}{2} \right\rceil$ then
        16: mark v as a detected wormhole attacker, and block any traffic from or to node v in future batches.
    17: end if
18: end for
```

Detect phase: Algorithm 2 represents the pseudo code of the detect phase of DAWN. For each node in the Detect phase, it receives reports from the judges nodes of any potential attackers. It first examines whether a report is from a valid judge node. if so, it will forward the report unless it has already been forwarded twice. Three-hops of the reports make sure that more (reachable) neighbors of the potential attacker will hear this report

(line 8) fig. 2 illustrates an example that a report is forwarded twice to make sure more neighbors receive it.

The detection algorithm on each node accumulates and calculates the number of its judge nodes who send report about the reported potential attacker in the current batch. If the number of judge nodes compose the majority (line 15), the node will make the decision that the attacker is involved in a wormhole attack and block it from future communications.

3.2.2 LOWER BOUND OF DETECTION RATE

In this section, we will show our proposed distributed algorithm DAWN can perform well with a high lower bound on detection rate. In particular, we have obtain the result in Theorem 1.

Theorem 1: *For any individual node v to be detected, let N (v) denote the set of the neighbors of v, and S(v) is the subset of n(v) s.t.*

$\forall\ w \in S(v), ETX(w)-ETX(v) > \delta$ (17)

here δ is the threshold. let n=|S(v)|, then the lower bound of the success rate of the algorithm is

$B = 1-\exp(-2np\left\lfloor -\frac{n}{2}\right\rfloor^2/n).$ (18)

Here p is the specified as equation (19):

$P=ETX(V) +\delta - 1/\ 2ETX\ (v) + \delta\ -1$ (19)

Proof: Based on the Theorem 1, one lower bound of the probabilities that one node in S(v) will receive the novel packets earlier than v equals to p in equation (19) by introducing the threshold δ. Thus, the success rate R satisfies

$R \geq \sum_{k=\left\lfloor\frac{n+1}{2}\right\rfloor}^{n} \binom{n}{k} P^k (1-P)^{n-k}$ (2 0)

TABLE 1

Lower bound B for different scenarios

ETX(V)	δ	n	B
5.0	9.0	39	98.66
5.0	8.0	49	98.97
5.0	10.0	41	99.38

The lower bound B can be determined by applying hoeffding's inequality [25]:

$R \geq \sum_{k=0}^{\left\lfloor\frac{n}{2}\right\rfloor} \binom{n}{k} P^k (1-P)^{n-k}$ (21)

$\geq 1-\exp\ (-2np\left\lfloor -\frac{n}{2}\right\rfloor^2/n)$ (22)

To illustrate the lower bound more clearly, we now show some numerical results with different settings. we may set proper n and δ for each node (i.e. n=41, δ=10.0, ETX = 5.0) in order to address the attacker successfully with a high probability near 1, as what Table 1 indicates.

3.2.3 COLLUSION RESISTANCE OF DAWN

The distributed detection algorithm DAWN requires the collaboration of the wormhole attackers neighbor nodes, i.e., monitoring attackers behavior, sending, forwarding and analyzing reports. It is possible that although these nodes do not participate in wormhole links, they collude with wormhole attackers by making false reports against honest nodes or other misbehavior in the report procedure to make the detection algorithm malfunction.

In this section, we analyze the resistance of DAWN against collusion in the report procedure. In particular, we obtain a condition on the number of colluding nodes, under which DAWN is resistant against colluding attacks, as stated in Theorem 2.

Theorem 2: *Let M be the set of the colluding nodes in the whole network. Then a necessary condition for DAWN to be resistant against colluding attacks is that Equation (23) holds for any node v:*

$|M \cap S(v)| < \lfloor S(v) + 1/2 \rfloor.$ *(23)*

Here S(v) is the same as in theorem 4.

Proof: Sketch: we prove by contra positive, i.e., if equation (23) does not hold, the decision error rate is not bounded. Supposed that DAWN is making a decision whether a is a wormhole attacker. If v is innocent, all the malicious nodes in S (v) can send false reports claiming v is involved in the wormhole attack. However, the number of the good nodes in S(v) who can send reports indicating v is innocent is specified as

$|S(v)\backslash M| < \left\lceil |S(V)| - \frac{1}{2}\right\rceil |M \cap S(V)|.$ (24)

Because it is the Same with the scenario that most nodes of s(v) is honest while v is malicious, it is impossible to judge whether v is malicious. For the case where v is a wormhole attacker and Equation (23) does not hold, simulation conclusion can be drawn.

For other scenario where the colluding nodes dominate the neighborhood of the wormholes attackers, since it falls out of the main scope of this paper, we omit the detailed solution here and leave it to future work.

IV. SIMULATION RESULTS

With the help of the parameters explained in the technical preliminaries, we find solution for the link that is affected by the wormhole attack. It also enhances the detection of innovative packets which is possibly done by DAWN.

Fig 3, shows the ratio of the packet delivery before a wormhole attack happens. This can be kept track with the help of ETX metric

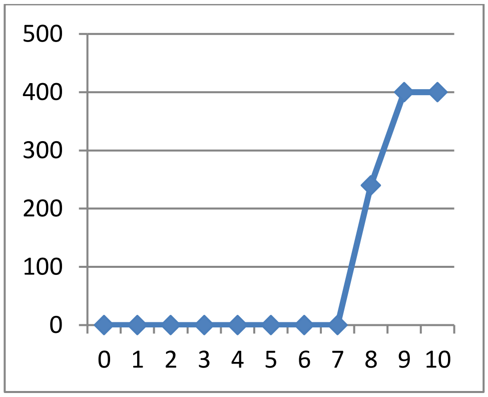

Fig 3: Shows the packet delivery ratio

Fig 4, shows how there are delay in packet transmission when affected by wormhole attack. It changes the path of the transmitted packets or helps in loss of packets which has to be sent to the destination.

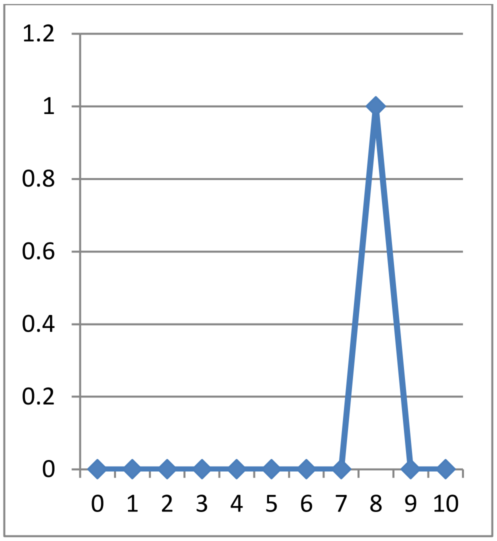

Fig 4: Shows the End to End Delay

After DAWN algorithm is applied, fig 5, shows how the algorithm is capable of detecting the wormhole attack and shows how it can be a apart of collusion-resistance.

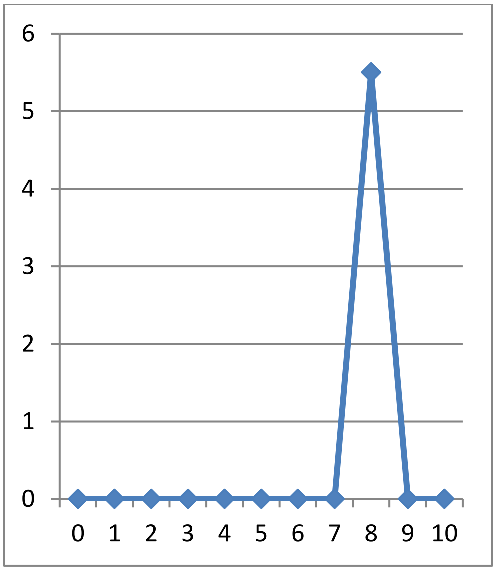

Fig 5: Shows Number of packets delivered finally

V. CONCLUSION

Since Wireless Sensor Networks are emerging as a promising platform in various fields, it is important to keep track o the arising security issues. By this paper, one can know how to detect the wormhole attack, what are the measures that can be taken in order to overcome the problem in the network. This approach helps in the field of Wireless Sensor Network which helps in controlling the network congestion arising through active attackers.

REFERENCES

[1] J. Ding, K. M. Sivalingam, R. Kashyapa. “A multi-layered architecture and protocols for large-scale wireless sensor networks,”Proc. IEEEVehicular Technology Conference (VCT2003), Orlando, USA, October 2003

[2] S. Datta , I. Stojmenovic “Internal node and shortcut based routing with guaranteed delivery in wireless networks,”Cluster Computing,vol.5, no. 2, pp. 169-178, 2002.

[3] J. Gao, L.J. Guibas, J. Hershberger, L. Zhang, and A. Zhu,“Geometric Spanners for Mobile Networks,” IEEE J. Selected Areas in Comm., vol. 23, no. 1, pp. 174-185, Jan. 2005.

[4] H. Frey, S. Ru¨ hrup, and I. Stojmenovic, “Routing in Wireless Sensor Networks,” Guide to Wireless Sensor Networks, S. Misra, I.Woungang, and S. C. Misra, eds., ch. 4, pp. 81-112, Springer-Verlag, May 2009.

[5] EEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 4, NO.2, MARCH/APRIL 2005A Location-Based Routing Method for Mobile Ad Hoc Networks Ljubica Blaze Vic, Member, IEEE, Jean-Yves Le Boudec, Fellow, IEEE, and Silvia Giordano, Member, IEEE

[6] M. Zorzi, ―A New Contention-Based MAC Protocol for Geographic Forwarding in Ad Hoc and Sensor Networks,‖ Proc. IEEE Int‘l Conf. Comm. (ICC ‘04),vol.6, pp. 3481-3485, June 2004.

[7] D. Son, A. H., And Krishnamachari, B. “The effect of mobility-induced location errors on geographic routing in mobile ad hoc and sensor networks: analysis and improvement using mobility prediction”.IEEE Trans. Mobile Comput. 3, 3 July 2004