ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 4, Issue 1 (Jan. - Mar. 2016)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2016)

Analyze and Detect Packet Loss for Data Transmission in Wireless Sensor Network

[I]Miriam Lakde, [II]Prof. Vaibhav Deshpande
[I,II]Dept. of CSE, St. Vincent Pallotti College of Engineering, Nagpur, Maharashtra, India

Abstract
Privacy-preserving routing is crucial for some ad hoc networks that require stronger privacy protection.
We achieve content un-observability by employing anonymous key establishment based on group signature. The unobservable routing protocol is executed in two phases. First, an anonymous key establishment process is performed to construct secret session keys. Then an unobservable route discovery process is executed to find a route to the destination.
In this protocol both control packets and data packets look random and indistinguishable from dummy packets for outside world. Only valid nodes can distinguish routing packets and data packets from dummy traffic with inexpensive symmetric decryption.
A node can establish a key with each of its neighbors, and then uses such a key to encrypt the whole packet for a corresponding neighbor.
The receiving neighbor can distinguish whether the encrypted packet is intended for it by trial decryption.MANET, due to the nature of wireless transmission, has more security issues compared to wired environments. In this paper we specifically considering Tunneling attack which does not require exploiting any nodes in the network and can interfere with the route establishment process. Instead of detecting suspicious routes as in previous methods, we implement a new method which detects the attacker nodes and works without modification of protocol, using a hop-count and time delay analysis from the viewpoint of users without any special environment assumptions.

Keywords
Security, Sensor Networks, Privacy, MANET, Packet Loss, Attacks.

I. Introduction

Mobile Ad hoc Networks (MANETs) are the special type of wireless network, where mobile nodes or terminals are connected through wireless interfaces forming a temporary network without any fixed infrastructure or a centralized administration. Mobile ad hoc networks are open to a wide range of attacks due to their unique characteristics like open medium, dynamically changing topology, and absence of Infrastructure, resource constraint (memory, bandwidth, computation power etc.) and trust among nodes. The principle behind mobile ad hoc networking is multi-hop relaying, which means messages sent by source to destination are forwarded by the other nodes if destination node is not directly reachable. MANETs are decentralized and therefore all network activities are carried out by nodes themselves. Each node is both an end-system as well as a relay node (router) to forward packets for other nodes. The routing algorithm designed for MANET such as AODV (Ad-hoc on-demand Distance Vector Routing) is based on the assumption that every node forwards every packet. But some of the nodes may act as the selfish nodes. These nodes use the network and its services but they do not cooperate with other nodes. Such selfish nodes or malicious nodes do not consume any energy such as CPU power, battery and also bandwidth for retransmitting the data of other nodes and they reserve them only for themselves.

In other words, an ad hoc node in MANET operates as not only end terminal but also as an intermediate router. Data packets sent by a source node may be reached to destination node via a number of intermediate nodes. Thus, multi-hop scenario occurs. In the absence of a security mechanism, it is easy for an attacker to insert, intercept or modify the messages. s including node impersonation, message injection, loss of confidentiality etc.

Privacy protection [10] of mobile ad hoc networks is more demanding than that of wired networks due to the open nature and mobility of wireless media. In wired networks, one has to gain access to wired cables so as to eavesdrop communications. In contrast, the attacker only needs an appropriate transceiver to receive wireless signal without being detected.

To achieve unobservability, a routing scheme should provide [10] unobservability for both content and traffic pattern. Hence we define refine unobservability into two types one is content Unobservability, referring to no useful information can be extracted from content of any message and another one is Traffic Pattern Unobservability, referring to no useful information can be obtained from frequency, length, and source-destination patterns of message traffic.

Our mechanism is to protect all parts of a packet's content, and it is independent of solutions on traffic [11] pattern unobservability. And it can be used with appropriate traffic padding schemes to achieve truly communication unobservability.

A wormhole attack is a particularly severe attack on MANET [12] routing where two attackers, connected by a high-speed off-channel link, are strategically placed at different ends of a network. These attackers then record the wireless data they overhear, forward it to each other, and replay the packets at the other end of the network. Our method selects routes and "avoids" rather than "identify" the wormhole resulting in low cost and overhead. We propose a multipath routing protocol called Multipath Hop-count Analysis efficient protocol which does not require any special supporting hardware. Furthermore, MHA [12] is designed to use split multipath routes, so the transmitted data is naturally split into separate route. An attacker on a particular route cannot completely intercept (and subvert) our content.

- We formulate the problem of secure provenance transmission in sensor networks, and identify the challenges specific to this context [13]
- We extend the secure provenance encoding scheme and devise a mechanism that detects packet drop attacks staged by malicious forwarding sensor nodes
- We perform a detailed security analysis and performance evaluation of the proposed provenance encoding scheme

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

and packet loss detection mechanism. [13]

II. Literature Survey

In 2006 K. Muniswamy-Reddy K. Muniswamy-Reddy, D. Holland, U. Braun, and M. Seltzer[2] et al, propose "Provenance- Aware Storage systems," .This survey states that in a multi-hop sensor network by using the data provenance scheme the BS can trace the source and forwarding path of an individual data packet. For each packet Provenance must be recorded but there is an important challenge arises due to the heavy storage, energy and bandwidth conditions of sensor nodes. So, it is necessary to provide a light-weight provenance scheme with low overhead.

In 2005 R. Hasan, R. Sion, and M. Winslett[4]et al proposes "Threat model for wireless sensor networks". The assumption about the BS is it should be a trusted one, but if any other arbitrary node may be attacked means the also be changed to malicious. An attacker can eavesdrop and perform traffic analysis anywhere on the path. In addition to this he/she is able to organize a few malicious nodes, as well as compromise/attack a few legitimate nodes by capturing them and physically overwriting their memory. If an attacker compromises a node means it can extract all key materials, data, and codes stored on that node. The adversary can drop, inject or alter packets on the links which are under the control of attacker. Also the attacker can create the denial of service attacks such as the complete removal of provenance. If a data packet does not contain any provenance records means it considered as highly suspicious data and hence generate an alarm/ signal at the BS about this malicious packet arrival. To overcome this type of detection the attacker attempts to misrepresent the data provenance

In 2012 S. Roy, M. Conti, S. Setia, and S. Jajodia, [5] et al propose "Secure Data Aggregation in Wireless Sensor Networks," .This work deals with attacks against the synopsis diffusion. This aggregation work presents a lightweight verification algorithm to make verification at the BS. The several synopses generated should be verified independently by the verification protocol at three phases. The phases are query dissemination phase, aggregation phase and the verification phase. In the first phase called query dissemination phase, the BS broadcasts the aggregation name to compute a random seed. In second phase called the aggregation phase, each node computes a sub aggregate value based on the local value and the synopses of its children. The node also randomly selects a set of MACs .From the selected MACs check whether it should be the received ones from its children.

Finally, in the third phase called verification phase, the BS computes the final synopses using the messages from its child nodes and verifies the received MACs.

In 2008 A. Ramachandran, K. Bhandankar, M. Tariq, and N. Feamster[7] et al proposed "Packets with Provenance" .This scheme catches provenance for network packets in form of per packet tags. The captured information stores a history of all nodes and processes that packet and manipulates those packets. However, this scheme assures a trusted environment which is not practical in sensor networks.

In 2010 W. Zhou, M. Sherr, T. Tao, X. Li, B. Loo, and Y. Mao[8] et.al proposes "Querying and Maintenance of Network Provenance at Internet- Scale" which describes the history and sub part of the network state. This result came from the execution of a distributed protocol. The disadvantage of this system is they does not address security concerns and is specific to some network use cases

In 2015, Ms. M. Tharani, Mr. K. Sivachandran and Ms. S. N. Saranya [9] et al proposed , "An Efficient Detection of Forgery and Packet Drop Attacks In Wireless Sensor Networks", which describes the survey addressing the problem of how securely transmitting provenance for sensor networks This survey plan proved beneficial in implementing a real system prototype of secure provenance scheme, to increase the accuracy of packet loss detection, especially in the case of multiple uninterrupted malicious sensor nodes.

In 2013, P. Thamizharasi and D.Vinoth [10]et al proposed, "Unobservable Privacy-Preserving Routing in MANET". This scheme proposed an efficient privacy-preserving routing achieving content unobservability by employing anonymous key establishment based on group signature. The disadvantage of this system is that they have only focused on security and full privacy preserved routing in mobile ad hoc networks have not been addressed

In 2014, K.G.S. Venkatesan R ,Resmi, R.Remya[11] et al proposed "Anonymizing Geographic Routing for Preserving Location Privacy Using Unlinkability and Unobservability " which describes a framework supporting anonymous location-based routing in certain types of suspicious MANETS. But the framework has not been extended to analytical model which captures the loss in node privacy due to the dynamics of the speed and the mobility patterns of nodes inside the MANET.

In 2009, Jen, Shang-Ming, Chi-Sung Laih, and Wen-Chung Kuo[12] et al proposed "A hop-count analysis scheme for avoiding wormhole attacks in MANET". This scheme instead of detecting wormholes from the role of administrators as in previous methods, they implement a new protocol, MHA, using a hop-count analysis from the viewpoint of users without any special environment assumptions. They provide four simulations to show the proposed scheme has high efficiency and very good performance with low overhead. In addition, this scheme does not require additional hardware or impractical assumptions of the networks. Hence, it can be directly used in MANET. The disadvantage of this system is that the dynamic information of the packets could still be modified.

In 2015 Salmin Sultana, Gabriel Ghinita, Elisa Bertino, and Mohamed Shehab[13] et.al proposes "A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks in Wireless Sensor Networks" which describes about the introduction of efficient mechanisms for provenance verification and reconstruction at the base station. In addition, they extend the secure provenance scheme with functionality to detect packet drop attacks staged by malicious data forwarding nodes. The disadvantage of this system is that the packet dropped by the malicious nodes through various attacks cannot be distinguished.

Table I. Summary

SRNO	TITLE	YEAR	AUTHOR	FACTS	FINDING
1	Provenance- Aware Storage systems	2006	K. Muniswamy-Reddy, D. Holland, U. Braun, and M. Seltzer	Multi-hop sensor network by using the data provenance scheme	Light-weight provenance scheme with low overhead.
2	Threat model for wireless sensor networks	2005	R. Hasan, R. Sion, and M. Winslett	Provenance records need to maintain	To keep the Base station secure from attackers
3	Secure Data Aggregation in Wireless Sensor Networks	2012	S. Roy, M. Conti, S. Setia, and S. Jajodia,	A novel collusion attack scenario against a number of existing IF algorithms	Makes IF algorithms not only collusion robust, but also more accurate and faster converging
4	Packets with Provenance"	2008	A. Ramachandran, K. Bhandankar, M. Tariq, and N. Feamster	Pedigree, a system for expressive, semantically-rich traffic classification	Allows network operators to leverage host-based trust models to decide treatment of network traffic
5	Querying and Maintenance of Network Provenance at Internet- Scale	2010	W. Zhou, M. Sherr, T. Tao, X. Li, B. Loo, and Y. Mao	ExSPAN, a generic and extensible framework	Achieves efficient network provenance in a distributed environment
6	An Efficient Detection of Forgery and Packet Drop Attacks In Wireless Sensor Networks	2015.	Ms. M. Tharani, Mr. K. Sivachandran and Ms. S. N. Saranya	Securely transmitting provenance for sensor networks	A real system prototype of secure provenance scheme, to increase accuracy of packet loss detection, especially in the case of multiple uninterrupted malicious sensor nodes.
7.	Unobservable Privacy-Preserving Routing in MANET	2013	P. Thamizharasi and D.Vinoth,	An efficient privacy-preserving routing protocol USOR	Achieves content unobservability by employing anonymous key establishment based on group signature.
8.	Anonymizing Geographic Routing for Preserving Location Privacy Using Unlinkability and Unobservability	2014	K.G.S. Venkatesan R , Resmi, R.Remya,	The framework which supports anonymous location-based routing in certain types of suspicious MANETS.	The framework works with any group signature scheme and any location-based forwarding protocol
9.	A hop-count analysis scheme for avoiding wormhole attacks in MANET	2009	Jen, Shang-Ming, Chi-Sung Laih, and Wen-Chung Kuo.	A novel scheme : MHA, based on an intuitive method to avoid wormhole attacks in MANET	Avoiding wormhole attacks from the viewpoint of users instead of the administrator's viewpoint
10.	A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks in Wireless Sensor Networks	2015	Salmin Sultana, Gabriel Ghinita, Elisa Bertino, and Mohamed Shehab	Light-weight provenance encoding & decoding scheme based on Bloom filters	Securely transmitting provenance for sensor networks

III. Proposed Methodologies

The unobservable routing protocol is executed in two phases [10]. First, an anonymous key establishment process is performed to construct secret session keys. Then an unobservable route discovery process is executed to find a route to the destination. In this protocol both control packets and data packets look random and indistinguishable from dummy packets for outside world. Only valid nodes can distinguish routing packets and data packets [10] from dummy traffic with inexpensive symmetric decryption. A node can establish a key with each of its neighbors, and then uses such a key to encrypt the whole packet for a corresponding neighbor. The receiving neighbor can distinguish whether the encrypted packet is intended for it by trial decryption. In order to support both broadcast and unicast, a group key and a pair wise key are generated.

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Our system comprises two phases:
Anonymous trust establishment
Unobservable route discovery

1) Anonymous Trust Establishment

In this phase, every node in the ad hoc network communicates [10] with its direct neighbors within its radio range for anonymous key establishment. Each node employs anonymous key establishment to anonymously construct a set of session keys with each of its neighbors.

2) Unobservable Route Discovery

This phase is a privacy-preserving route discovery process based [10] on the keys established in previous phase. Similar to normal route discovery process, our discovery process also comprises of route request and route reply.
Under the protection of these session keys in the first phase, the route discovery process can be initiated by the source node to discover a route to the destination node.
This proposed routing protocol has been implemented by the Network Simulator2 (NS2).
The Network Simulator is mainly utilized to implement the routing protocols in the networking research. The Main focus of our analysis is security and privacy. Attacks that prevent and detect the wormhole attack are most commonly known as packet leashes mechanism. In this paper, they are presented two types of leashes: geographic leashes and temporal leashes [14] also presented an authentication protocol. The authentication protocol is named as TESLA with instant key disclosure and this protocol, for use with temporal leashes. In, geographic leashes each node access GPS information and based on loose clock synchronization. Whereas temporal leashes require much tighter clock synchronization (in the order of nanoseconds), but do not tightly depend on GPS information and temporal leashes that are implemented with a packet expiration time.

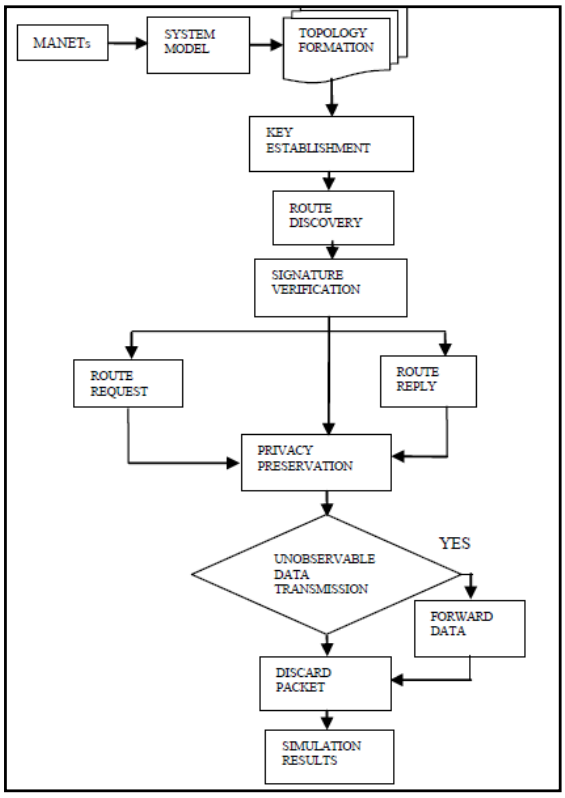

Fig : System Flow Diagram of Proposed System.

The observation of this scheme is geographic leashes are less efficient than temporal leashes, due to broadcast authentication, where precise time synchronization is not easily achievable.

IV. Expected Out-Come

The implementation result gives acceptable performance in terms of packet delivery ratio, packet delivery latency. But this protocol achieves anonymity, complete unlink-ability, unobservability in terms of content and traffic and more over resists completely against the attacks thereby minimizing the greater vulnerability of attacks.
For wormhole attack the simulation we will created node models, process models, & packet models, we will used some predefined node models from library. The details of models with their technical parameters are as follows

Total Nodes = 50
Infected node=6
Packet size = 1024 bits constant
Applying protocol=DSDV

We will perform the simulation of the proposed scheme in Network Simulator2 (NS2) to prove practical efficiency of the scheme. The steps of modeling in FSM [14] (Finite State Machine) of Proposed Algorithm are as follows:
Step1. Randomly Generate a Number in between 0 to maximum number of nodes.
Step2. Make the Node with same number as transmitter node.
Step3. Generate the Route from selected transmitting node to any destination node with specified average route length.
Step4. Send packet According to selected destination and start timer to count hops and delay.
Step5. Repeat the process and store routes and their hops and delay.
Step6. Now if the hop count for a particular route decreases abruptly for average hop count then at least one node in the route must be attacker.
Step7. Now check the delay of all previous routes which involve any on node of the suspicious route. Now the node not encounter previously should be malicious let there are N such nodes.
Step8. In N == 1 then it is the attacker else wait for future sequences which shows deviation and involve only one of N nodes.
Step9. These nodes are black listed by the nodes hence they are not involved in future routes.
Step10. Whole process (from step1 to step9) is repeated until we didn't get the specified goal (goal can be [14]

1. To get complete list of malicious nodes.
2. To run for specified time.
3. To run for specific number of packets etc.

V. Conclusion

In this paper we have described our survey over various packet loss and security approaches and also proposed a light-weight provenance encoding and decoding scheme based on Unobservable route discovery protocol to prevent packet loss in case malicious sensor nodes.

References

[1] *I. Foster, J. Vockler, M. Wilde, and Y. Zhao, "Chimera: A Virtual Data System for Representing, Querying, and*

Automating Data Derivation," Proc. Conf. Scientific and Statistical Database Management, pp. 37-46, 2002.

[2] K. Muniswamy-Reddy, D. Holland, U. Braun, and M. Seltzer,"Provenance-Aware Storage systems," Proc. USENIX Ann. Technical Conf., pp. 4-4, 2006.

[3] C. Rothenberg, C.Macapuna,M.Magalhaes, F. Verdi, and A. Wiesmaier, "In-Packet Bloom Filters: Design and Networking Applications," Computer Networks, vol. 55, no. 6, pp. 1364-1378, 2011.

[4] R. Hasan, R. Sion, and M. Winslett, "The Case of the Fake Picasso: Preventing History Forgery with Secure Provenance," Proc. Seventh Conf. File and Storage Technologies (FAST), pp. 1-14, 2009.

[5] S. Roy, M. Conti, S. Setia, and S. Jajodia, "Secure Data Aggregation in Wireless Sensor Networks," IEEE Trans. Information Forensics and Security, vol. 7, no. 3, pp. 1040-1052, June 2012.

[6] Y. Simmhan, B. Plale, and D. Gannon, "A Survey of Data Provenance in E-Science," ACMSIGMOD Record, vol. 34, pp. 31- 36, 2005.

[7] A. Ramachandran, K. Bhandankar, M. Tariq, and N. Feamster, "Packets with Provenance," Technical Report GT-CS-08-02, Georgia Tech, 2008.

[8] W. Zhou, M. Sherr, T. Tao, X. Li, B. Loo, and Y. Mao, "Efficient Querying and Maintenance of Network Provenance at Internet- Scale," Proc. ACM SIGMOD Int'l Conf. Management of Data, pp. 615-626, 2010. 2011.

[9] Ms. M. Tharani, Mr. K. Sivachandranand Ms. S. N. Saranya. "An Efficient Detection of Forgery and Packet Drop Attacks in Wireless Sensor Networks."IJAICT ISSN 2348 – 9928 Volume 2, Issue 7, November 2015.

[10] P. Thamizharasi and D.Vinoth, "Unobservable Privacy-Preserving Routing In MANET",in IJESE, ISSN: 2319–6378, Volume-2, Issue-3, January 2013

[11] K.G.S. VenkatesanR ,Resmi, R.Remya, "Anonymizing Geographic Routing for Preserving Location Privacy Using Unlinkability and Unobservability" in IJACSSE, Volume 4, Issue 3, March 2014

[12] Jen, Shang-Ming, Chi-Sung Laih, and Wen-Chung Kuo. "A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET", Sensors 9.6 (2009): 5022-5039.

[13] Salmin Sultana, Gabriel Ghinita, Elisa Bertino, and Mohamed Shehab, " A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks in Wireless Sensor Networks journal of latex class files, vol. 6, no. 1, january 2007" IEEE transactions on depedable and secure computing. pp256 – 269, 2015

[14] PushpendraNiranjan, PrashantSrivastava, Raj kumarSoni, Ram Pratap, "Detection of Wormhole Attack using Hop-count and Time delay Analysis" International Journal of Scientific and Research Publications, Volume 2, Issue 4, April 2012 1 ISSN 2250-3153

[15] W. Zhou, Q. Fei, A. Narayan, A. Haeberlen, B. Loo, and M. Sherr, "Secure Network Provenance," Proc. ACMSOSP, pp. 295-310, 2011.

[16] T. Wolf, "Data path credentials for high-performance capabilities based networks." in Proc. of ACM/IEEE Symp. on Architectures for Networking and Communications Systems., 2008, pp. 129–130.

[17] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in Proc. of Intl. Workshop on Sensor Network Protocols and Applications, 2003, pp. 113–127

[18] S. Papadopoulos, A. Kiayias, and D. Papadias, "Secure and efficient in-network processing of exact sum queries," in Proc. of International Conference on Data Engineering, 2011, pp. 517–528.

[19] S. Sultana, E. Bertino, and M. Shehab, "A provenance based mechanism to identify malicious packet dropping adversaries in sensor networks," in Proc. of ICDCS Workshops, 2011, pp. 332–338.