International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 01 (JAN-FEB, 2016)

A Survey of Secure Routing in Mobile Ad-hoc Network

Utsav Singhi
M. Tech. Scholar Department of CSE
RKDF, University, Bhopal, M.P., India
singhiutsav@gmail.com

Prof. Gagan Sharma
HOD Department of CSE
RKDF, University, Bhopal, M.P. India
gagansharma.cs@gmail.com

***Abstract*--Security of wireless mobile sensor network becomes crucial key factor in the latest research available in the fast deployment of wireless sensor network. The time interval between an attack detection and corrective action taken by the administrator in a system is usually high and therefore, at the time the administrator notices an attack and takes some suitable action the damage was done by the attacker. Depending on this scenario the need for Intrusion Detection System which can not only detect various types of attacks but also be able to actively respond against malicious activities is required. Intrusion detection is a preemptive approach in a system security which is used to identify malicious activities and respond quickly to mitigate anomalous behavior. In this research paper we actively proposed a new and efficient approach in intrusion detection by neighbor trust methodology based communication establishment. We define the basics of intrusion detection in wireless network by describing the varieties of attacks and state the motivation for intrusion detection in wireless network. In this paper, we proposes an IDS which is based on node monitoring technique and is able to detect selective forwarding attacks or routing attack and also able to eliminate the postulates of security algorithm by using trust calculation algorithm.**

Keywords- WSN, IDS, attacks, Watchdog Monitoring Technique

I. Introduction

The wireless sensor networks (WSNs) are often deployed in physically insecure environment where we can hardly prevent attackers from the physical access to the devices. Since making nodes resistant to physical tampering would make them much more expensive, we have to think that an attacker may capture the nodes and retrieve the cryptographic material via physical tampering [1, 2, 3]. A wireless IDS may aid within the detection of a variety of attacks. Not solely will a wireless IDS Sight knave WAPS, determine non-encrypted 802.11 traffic, associate degree facilitate isolate an attacker's physical location, as mentioned earlier - a wireless IDS will cite several of the quality (and not-so standard) wireless attacks and probes still. In an attempt to spot potential WAP targets, hackers ordinarily use scanning computer code. Hackers or curious people can use tools like Nets tumbler or Kismat to plan a given area's WAPs. Utilized in conjunction with a worldwide Positioning System (GPS) these scans not solely find WAPs. However additionally log their geographical coordinates. These tools became thus well-liked that they're square measure websites dedicated to mapping the world's WAP earth science. A wireless IDS will cite these and other scans, serving two to boost awareness of the threats to the wireless fidelity. A

International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 01 (JAN-FEB, 2016)

wireless network could be a wireless network consisting of spatially distributed autonomous devices exploitation sensors to hand in glove monitor physical or environmental conditions, like motion, temperature, pressure, sound, vibration, , or pollutants, at completely different locations the event of wireless networks was originally driven by military applications like field of battle police investigation.

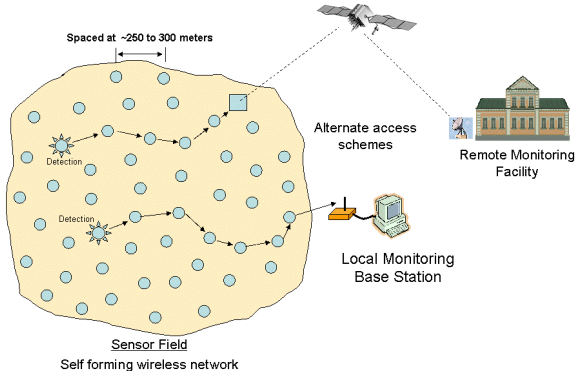

Figure 1.1: Wireless Sensor Network

However, wireless networks square measure currently utilized in several civilian application areas, as well as setting and surround observance, control, home automation, and health care applications. Wireless sensor network refers to a system that consists of variety of inexpensive, resource restricted detector nodes to sense vital information associated with setting and to transmit it to sink node that gives entrance way practicality to a different network, or associate degree access purpose for human interface. Wireless sensor network could be a speedily growing space as new technologies square measure rising, new applications square measure being developed, like traffic, setting observance, healthcare, military applications, home automation. A wireless network is susceptible to numerous attacks like jam, battery avoidance, routing cycle, Sybil, cloning. Thanks to limitation of computation, memory and power resource of detector nodes, advanced security mechanism can't be enforced in Wireless sensor network. So energy-efficient security implementation is a very important demand for Wireless network to protect Wireless network against completely different varieties of vulnerabilities, preventive mechanisms like cryptography and authentication will be applied to stop some sorts of attacks. This sort of preventive mechanisms fashioned the primary defense line for Wireless network. However, some attacks like wormholes, sinkhole, couldn't be detected exploitation this sort of preventive mechanisms. Additionally, these mechanisms square measures solely effective to stop from outside attacks and didn't guarantee the interference of intruders from within the network (Silva et al., 2005). Due to that, it's necessary to use some mechanisms of intrusion detection. Intrusion Detection Systems (IDS) square measure thought of to act because the second defense line against network attacks that preventive mechanisms fail to deal with (Silva et al., 2005). Associate degree Intrusion detection system is outlined in (Debar et al., 1999) .A system that dynamically monitors the events going down on a system associate degreed decides whether or not these events square measure symptoms of an attack or represent a legitimate use of the system. However, there square measure several challenges posed against the appliance of the IDS for Wireless network. These challenges square measure thanks to the dearth of resources like, energy, process and storage. Wireless networks square measure assortment of nodes wherever every node has its own detector, processor, transmitter and receiver and such sensors sometimes square measure low price devices that perform a selected variety of sensing task. Being of low price such sensors square measure deployed densely throughout the world to

International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 01 (JAN-FEB, 2016)

watch specific event. The Wireless network largely operates publicly and uncontrolled space gives a chance to intruder to trespass the safety of an application. Today Intrusion used as a security resolution in a much wired sensor network within the type of software/ hardware by that one will sight unwanted services happening the system by approach of enhanced/abnormal network activity and determine suspicious patterns that will indicate whether or not the network/system is beneath attack? For Wireless sensor network many schemes were projected however they need restricted options like solely concern to attacks on a specific layer.

II. IDS Fundamentals in WSN

We introduce the basics of the intrusion detection in Wireless network, which has the definition of the intrusion, kinds of intrusions/attacks in Wireless network, the motivation and want for intrusion detection and therefore the challenges of developing an honest candidate intrusion detection theme for Wireless network. The definition of the Intrusion/Attack: Heady (1990) et al. [4] defines the intrusion as any set of actions that try to compromise the most parts of the safety system: the integrity, confidentiality or handiness of a resource. Within the same work, the interloper so was outlined as a personal or cluster of people WHO take the action within the intrusion. Zamboni (2001) et al. [5] adds the statement of success or failures of those actions thus it additionally refers to the attacks against the pc system. Within the theme of wireless detector network, the conception stills constant since the intrusion additionally target any of the parts mentioned on top of. The character of Wireless network and its special characteristics just like the harsh readying, energy constraints and therefore the media of communication makes them terribly liable to the intrusions quite different networks.

1. Types of Intrusion Detection System

There are two types of approaches based on the detection technique in wireless sensor network: Misuse Detection also referred to as Signature based Intrusion Detection (SID) and Anomaly based Intrusion Detection (AID). In SID detection, each network traffic record is recognized as either normal or one of many predefined intrusion types. In contrast, anomaly detection amounts to training models for learning normal traffic behavior and then classifying, as intrusions, any network behavior that considerably deviates from the known normal network traffic patterns. Intrusion signatures have been characterized as a string, event sequences, graphs, and intrusion scenarios (consisting of target states, event sequences, and their preconditions). FSM (finite-state-machine), colored Petri Nets, associate rules and production rules of expert systems have been used to represent and recognize intrusion signatures. Intrusion signatures are either physically encoded or manually learned through data mining. But, signature recognition techniques have a limitation in that they cannot detect original intrusions whose signatures are unknown.

2. Types of attacks in Wireless network

- Outsider versus business executive attacks supported the node that's launching the attack, if it happiness to the network thus it's thought-about as business executive attack, otherwise it's thought-about as outsider attack.
- Passive versus active attacks supported the impact that results from AN attack. Passive attacks simply monitor or pay attention to the info packets, whereas

the active attacks do modify the info streams or according false alarms to the bottom station.

- Mote-class versus laptop-class attacks supported the potential of the wrongdoer in compromising the network. In mote-class attacks, some nodes with an analogous capability to the network nodes are used as attackers, whereas in laptop-class, uses powerful devices like laptops with higher transmission varies, processing power and energy to compromise the network.

III. Related Work

In MANETs security is the major concern in applications such as communication and data sharing. These are so many chance s of different types of attacks due to self- organizing property of MANETs. Malicious attacker may try to attack t h e data packets by tracing the route. They may try to find the source and destination through different types attacks. MANETs are vulnerable to malicious attackers that target to damage and analyze data and traffic analysis by communication eavesdropping or attacking routing protocols. Anonymous routing protocols are used by MANETs that hi de s the identity of nodes as well as routes from outside observers. In MANETs anonymity means identity and location anonymity of data sources and destinations as well as route anonymity. However existing anonymous routing protocols have significantly high cost, which worsens the resource constraint problem in MANETs. The [6] paper proposes Secured Hierarchical Anonymous Routing Protocol (SHARP) based on cluster routing. SHARP offers anonymity to source, destination, and routes. Theoretically SHARP achieves better anonymity protection compared to other anonymous routing protocols. ALARM [7] (Anonymous Location-Aided Routing) requires off-line group manager (GM) that initializes the underlying group signature system that enrolls all authentic nodes as group members. In case of a dispute, the GM is responsible for opening the contested group signature and determining the signer. The GM may also have to handle upcoming joins for new ones as well as cancellation of existing members. Each node broadcast its LAM (Location Announcement Message). Each node that receives a LAM, it verifies group signature. The node broadcasts the message to its neighbors if it is valid signature. After getting the LAM each node maintain a map and connectivity graph. When a node wanted makes a communication it checks whether a node is present in that position. Then it sends message to that destination using its pseudonym. The sending message is encrypted using the public key in its LAM. ARM (Anonymous Routing Protocol for Mobile Ad hoc Networks) hides routes in the network against passive global and local attacks. Nodes inside the network will not be able to determine that whether it receives the message from actual source or from forwarder due to probability padding. It hides the actual path between source and destination in a cloud. This protocol doesn't require any cryptographic operations. ALERT [8] is another anonymous routing protocol which is zone based. Here the entire network is divided into zones such that sender and receiver are not in the same zone. The routing procedure is based on GPSR protocol. The forwarding node is the neighbor which is very close to the destination. To protect the node identities each node uses the dynamic pseudonyms instead of their original identities. To provide the source anonymity it uses notify and go mechanism. The destination is protected by local broadcast and multicast. There are so many such existing anonymous routing protocols. Some of them are location

based. ALARM, ALERT, PRISM are some of the examples. ALERT, ZAP are zone based protocols. ANODR and DASR are based on cryptographic techniques. MASK uses pseudonyms to ensure the anonymity. Most of them can't provide the full anonymity together. ALARM cannot provide the location of sender and receiver, SDDR lacks the route privacy, and ZAP concentrates only on destination privacy. Some existing works does not support route anonymity. Most of them generate high cost. Blaze, Feigenbaum, and Lacy [9] firstly introduce trust management as a separate component of security services and give an overall definition of the trust management problem. The authors propose a unified decentralized trust management system, policymaker, which was based on a simple language for describing security policies, credentials and relationships. New trust scheme is necessary to the special characteristics of the sensor network. Reputation-based Framework for Sensor Networks (RFSN) [10] is the reputation and trust-based model designed and developed exclusively for sensor networks, which using watchdog mechanism to build trust rating. Each sensor node develops a reputation for each other node by making direct observations about the other neighbor nodes. This reputation is used to help a node evaluate the trustworthiness of other sensor nodes and make decisions within the network. But the watchdog cannot record all the behavior due to its own fault or network error, so there is some uncertainty events in the trust system. Mutual entity authentication plays an important role in securing wireless sensor networks. Zhijun Li and Guang Gong propose a computationally efficient authentication framework, based on a well-studied problem—learning parity with noise (LPN). This kind of LPN-based authentication approach only involves simplest bit operations, which makes them suitable for resource restrained sensor nodes. The proposed framework introduces a new noise mode to prevent a general man-in-the-middle attack. Haiguang Chen and Huafeng propose agent-based trust management model system to enforce the security of wireless sensor networks [11]. The agent nodes monitor the behavior of sensor nodes within its radio range to distribute the trust rating. They don't need the second-hand information to build trust system. Research in securing MANETs has to date mostly focused on detecting and preventing specific attacks. For example TOGBAD was proposed in [12] to identify nodes that attempt to create black hole attacks in MANETs that use the OLSR routing protocol. Kurosawa and Jamalipour [13] also propose a black hole detection mechanism, this time for AODV. Xiaopeng and Wei [14] proposed a grey-hole attack detection scheme for the DSR routing protocol. Ping and Zhang [15] considered a route request (RREQ) flooding attack in MANETs. They proposed a RREQ flooding prevention mechanism based on neighbor's supervision. In [16] Perrig and Johnson analyzed how an attacker can launch a rushing attack (RU) in DSR and proposed a rushing attack prevention mechanism for MANETs. Though most researchers have concentrated on protecting MANETs against specific types of attack, some have suggested a more general approach. For example ARAN [17] is a hop-by-hop authenticated routing mechanism that can protect MANETs against a number of attacks from external malicious nodes. A similar approach, Ariadne [18] has been proposed for end-to-end authentication based on shared key pairs. We believe more effort is needed on mechanisms which can guard MANETs against a wide variety of attacks. Methods proposed in [17] & [18]

protect MANETs mainly against external attackers through authenticated routing. However an insider trusted node can change its behavior and initiate activities.

VI. PROPOSED WORK

In this paper we study number of research papers and identifies that security is measure concerned in MANET, in our proposed work we provide efficient security mechanism against routing attack, for that purpose we apply neighbor trust based security mechanism are used, during the communication while any node identified as a attacker than we apply trust calculation methodology, in this scheme we calculate percentage of performance of every node, based on incoming and outgoing data transmission, and while any node performance lower than the threshold percentage, then we check the packet forwarded by the intermediate node and identifies their behavior. Those neighbor trust mechanisms are light weighted security mechanism and provide secure communication against routing attack in MANET.

V. CONCLUSION

Here we study the intrusion detection problem by characterizing intrusion detection probability with respect to the intrusion distance and the network parameters (i.e., node density, sensing range, and transmission range).The analytical model for intrusion detection allows us to analytically formulate intrusion detection possibility within a certain intrusion distance under various application scenarios in future. Once we find the intruders than technique is used to stop intruders using neighbor trust mechanism. Our Intrusion Detection System also implement in mobile ad-hoc network application and parallel computer interconnection network.

REFERENCES

[1] Y. Zhang,G. chen, W. Weng, and Z. Wang, “An Overview of Wireless Intrusion Prevention Systems ”IEEE *ICCSNA* , vol. 3, no. 12, pp. 147–150, 2010.

[2] K. Suresh, A. Sarala Devi, and Jammi Ashok, “A Novel Approach Based Wireless Intrusion Detection System”, IJCSIT, Vol. 3 (4), 2012, 4666 – 4669, ISSN: 0975-9646.

[3] Heady, R., 1990. The Architecture of a Network-level Intrusion Detection System.1st Edn., Department of Computer Science, Mexico, pp: 18.

[4] Zamboni, D., 2001. Using internal sensors for computer intrusion detection. Purdue University.

[5] Debar H. M. Dacier and A. Wespi, 1999. Towards at taxonomy of intrusion-detection systems. Comput Netw., 31: 805-822.

[6] Remya S, Lakshmi K S, “SHARP: Secured Hierarchical Anonymous Routing Protocol for MANETs”, 2015 International Conference on Computer Communication and Informatics (ICCCI -2015), Jan. 08 – 10, 2015, Coimbatore, INDIA.

[7] K.E. Defrawy and G. Tsudik,”ALARM: Anonymous Location- Aided Routing in Suspicious MANETs,” Proc. IEEE Intl Conf. Network Protocols (ICNP), 2007.

[8] Haiying Shen and Lianyu Zhao,”ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs”, Proc. Intl Conf. Parallel Processing (ICPP), 2011.

[9] M. Blaze, J. Feigenbaum, and J. Lacy. Decentralized trust management. In Proceedings of the 1996 IEEE Symposium on Security and Privacy: 164-176

[10] S. Ganeriwal and M. Srivastava. Reputation-based framework for high integrity sensor networks. In

Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN '2004): 66-77

[11] Zhijun Li and Guang Gong. Computationally efficient mutual entity authentication in wireless sensor networks. Ad Hoc Networks.2011, 9(2): 204-215.

[12] E. Padilla, N. Aschenbruck, P. Martini, M. Jahnke and J. Tolle, "Detecting Black Hole Attack in Tactical MANETs using Topology Graph", Proceedings of 32nd IEEE Conference on Local Computer Networks, 2007.

[13] S. Kurosawa and A. Jamalipour, "Detecting Black-hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, November 2007.

[14] G. Xiaopeng and C. Wei, "A Novel Grey Hole Attack Detection Scheme for Mobile Ad-Hoc Networks", Proceedings of IFIP International Conference on Network & Parallel Computing, 2007.

[15] P. Yi, Z. Dai and S. Zhang, "Resisting Flooding Attack in Ad Hoc Networks", Proceedings of IEEE Conference on Information Technology: Coding and Computing", Vol.2, pp 657-662, 2005.

[16] Y.Hu, A. Perrig and B. Johnson, "Rushing Attack and Defense in Wireless Ad Hoc Networks Routing Protocols", Proceedings of 2nd ACM workshop on Wireless Security, New York, 2003.

[17] K. Sanzgiri and M. Belding-Royer, "A Secure Routing Protocol for Ad Hoc networks", Proceedings of 10th IEEE International Conference on Network Protocol 2002, (ICNP' 02).

[18] Y.Hu, A. Perrig and B. Johnson, "A Secure On Demand Routing Protocol for Ad Hoc networks", Proceedings of MobiCom, Atlanta, Georgia, USA, pp 23-28, September 2002.