International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Survey on Secure and Reliable Data Routing in WSN

Trupti Anil Bomble[1], M. D. Ingle[2]

[1]ME Computer (Engineering), Jayawantrao Sawant College of Engineering, Hadapsar, Pune-28, Savitribai Phule Pune University, Pune, India

[2]Professor, Computer Engineering, Jayawantrao Sawant College of Engineering, Hadapsar Pune-28, Savitribai Phule Pune University, Pune, India

Abstract: ***Wireless Sensor Networks (WSNs) are materializing as one of the dominant technologies of the future because of their large range of applications in military and civilian fields. Because of their operating behavior, they are often neglected and thus vulnerable to various types of attacks. For instance, an attacker could catch sensor nodes, getting all the information saved therein—sensor nodes are generally considered to not be tamper-proof. Hence, an attacker may clone catched sensor nodes and use them in the network to conduct a variety of mischievous activities. As the decisions taken by a sensor network rely on the information gathered by the sensor nodes, if an adversary inhibits the necessary or confidential data from being forwarded to the BS/ target, this will cause the whole breakdown of the network or outcomes in the wrong judgment being made, possibly causing deliberate loss. There are many types of attacks such as compromised node, denial of service attack, black hole attack, etc. Hence there is a necessity to find all such attacks in WSN, and to safely route our sensitive information to the target. This paper represents the survey of some types of attack and there detection techniques. Also the survey includes different techniques for secure and reliable data collection in Wireless Sensor Networks.***

Keywords: Wireless Sensor Networks, Network lifetime, Security, Trust, Attacks

1. Introduction

Wireless Sensor Networks (WSNs) are materializing as a encouraging technology because of their large range of uses and applications in industrial, environmental watching, military and civilian fields. Because of economic deliberation, the sensor nodes are commonly simple and of less cost.

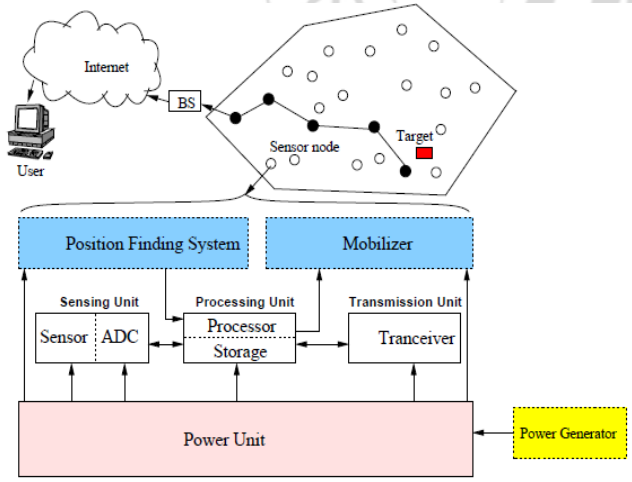

Figure 1: Components Of sensor nodes

Figure 1 shows the structural diagram of sensor node components. Generally, sensor node consists of sensing, processing, transportation, mobilizer, position detecting system, and power units. The same diagram represents the communication structure of a WSN. Sensor nodes are basically dispersed in a sensor field, which is the region where the sensor nodes are placed. Sensor nodes cooperate between themselves to generate good-quality information about the physical surroundings. Every sensor node takes its decisions on its goal, the data it presently has, and its familiarity of its computing, communication, and power resources. Each of these dispersed sensor nodes has the ability to gather and forward information either to other sensor nodes or back to an outside base station. A base station may be a static node or a dynamic node which is capable of connecting the wireless sensor network to an already presented communications structure or to the network where a user can have entry to the reported information.

In the working of Wireless Sensor network, the sensor nodes are often neglected, nevertheless, and are thus likely to go through from various types of novel attacks such as compromised node attack, Denial of service attack, Black hole attack, etc. A black hole attack (BLA) is one of the most basic and common type of attacks, in which the attacker captures a sensor node and drops all data packets that are forwarded through this sensor node, concluding in important and sensitive data being rejected or not able to be forwarded to the BS/ target. Because the network comes on the conclusion depending on the sensor nodes' captured data, the aftermath is that the network will totally break and, more seriously, take wrong decisions. And hence, how to find and prevent BLA is of great implication for security in WSNs.

2. Related Work

In this paper [1], authors have proposed active detection-based security and trust routing technique for wireless sensor network called as ActiveTrust. In this, numbers of detection routes are actively created to immediately detect and calculate nodes trust values in order to enhance the data packet route security. More necessarily, the creation and dispersion of detection routes are introduced in the ActiveTrust technique, which can entirely use the power in non-hotspots to generate as many detection paths as required to obtain the expected security and power efficiency. Both

exhaustive hypothetical monitoring and experimental results shows that the working of the ActiveTrust technique is better as compared to existing techniques. ActiveTrust can considerably enhance the data route accomplishment probability and capability opposed of black hole attacks and can increase the network lifespan.

In this paper [2], author has introduced a multi dataflow topologies (MDT) strategy to confront the SFA i.e. selective forwarding attack. In the MDT strategy, the network is isolated into two dataflow topologies. Alike if one topology has a mischievous sensor node, the BS can still receive data packets via other topology.

The MDT strategy can find the mischievous sensor nodes. When the Sink or base station drops some packets, it will pinpoint all probable areas that the mischievous sensor nodes may be distributed in. Following that, the base station can collect and monitor the information about all probable lost areas; thus the base station can use the information to detect the mischievous sensor nodes.

Also the MDT strategies do not require to obtain its geological location. In the MDT strategy, the base station only require to recognize the probable areas that the sensor nodes may be placed in if the base station wish to locate the mischievous sensor nodes.

In this paper [3], authors have introduced a hybrid multipath scheme (H-SPREAD) to enhance both security and reliability. H-SPREAD integrates the proposed path formation process in N-to-1 Multipath Routing Protocol in addition to a hybrid message transportation scheme to enhance the reliability and security of data transportation in wireless sensor networks. HSPREAD holds the benefits of a threshold secret sharing technique and route diversification of multipath data promoting to boost path flexibility against node breakdown or compromise routes. As per the invulnerable property of the threshold secret distribution technique, data packets can be protectively forwarded on the way to the sink node even when a short number of sensor nodes or routes have breached or are attacked during the data transportation process.

In this, the source node splits every data packet to the various shares, S1, S2, S3… Sn, and then sends them on the way to the BS via different paths. Based on the specific disparateness of the threshold secret distribution technique, even when some number of routes has broken due to link or node breakdown, the distinct communication can still be recapture through other obtained shares at the target node.

N-to-1 Multipath Routing Protocol is introduced as per the converge cast traffic pattern of WSN. The core aim is to locate numerous node-disjoint routes from all the sensor nodes on the way to a sink node. In extension, via data transportation step, all the transitional nodes use packet recover technique at each node to enhance data transportation reliability. In spite of, since this way uses the N-to-1 multipath routing algorithm to build various routes, this protocol may goes from the effects of wireless barrier. Hence, large packet drop ratio caused by barrier can decrease the possibility of successful packet recovery at the sink sensor node. Furthermore, H-SPREAD enhances perseverance and security of data deployment in the network, but it cannot enhance security of distinctive nodes.

In this paper [4], a Per-Hop Acknowledgement (PHACK)-based technique is introduced for every packet transposition to find selective forwarding attacks. Here, the BS and every sensor node along the prolonging path produces an acknowledgement (ACK)/ feedback message for every obtained packet to certify the ordinary packet transmission. The scheme, in which every ACK message is revert to the sending sensor node along a disparate routing path, can considerably enhance the flexibility against attacks because it prohibits an adversary from compromising sensor nodes in the restoration routing path, which can alternatively intrude the return of sensor nodes' ACK message. The PHACK technique also has superior capability to find anomalous packet loss and detect doubtful nodes as well as superior flexibility against attacks. Other central issue is the network lifespan of the PHACK technique, as it produces more acknowledgement messages than past ACK-based techniques. It is observed that the network lifespan of the PHACK technique is not less than that of another ACK-based technique because the technique just enhances the power utilization in non-hotspot regions and does not enhance the power utilization in hotspot regions. Furthermore, the PHACK technique largely clarifies the protocol and is simple to implement. Both intellectual and simulation outcomes are given to determine the efficiency of the introduced technique in terms of large detection possibility and the capability to find doubtful sensor nodes.

In this paper [5], authors have introduced a randomized multi-path routing procedure. This algorithm estimates various paths in a arbitrary manner every time an information packet wish to be transmit, such that the set of paths taken by multiple shares of distinct packets keep altering over time. As an outcome, a more number of routes can be possibly produces for each source and target. To interrupt various packets, the attacker has to compromise or trouble all probable routes from the source node to the target node, which is virtually impractical.

Here authors have achieved the goal by introducing four dispersed schemes for inseminating information "shares": purely random propagation (PRP), directed random propagation (DRP), non-repetitive random propagation (NRRP), and multicast tree-assisted random propagation (MTRP).

In this paper [6], authors have exposed the ineffective utilization of watchdog mechanism in currently available trust systems, and by that proposed a series of escalation methods to reduce the energy expenditure of watchdog usage, while maintaining the system's security in a satisfactory level. Authors' donation subsists of hypothetical analyses and practicable algorithms, which can conveniently and effectively line up the watchdog job depending on the sensor nodes' position and the destination nodes' truthfulness.

The watchdog technique is reformed in two levels. First, watchdog locations are reformed by seeing the fact- despite

the sensor nodes that are placed more nearly may utilize less power to observe each other because of smaller communication range; these sensor nodes are more hopeful of being negotiate together and perform coordinated attacks. Hence optimal watchdog position (given a destination node) is explored to reduce the comprehensive risk (in terms of power utilization and security). Second, watchdog frequency is optimized and decreased its repetition.

In this paper [7], authors have proposed a new trusted path which considers communication reliability and route length for a reliable and feasible date packet delivery in a MANET. In most of the MANET routing techniques, security is extra layer above the routing layer. Authors have proposed the term called attribute similarity in detecting possibly friendly sensor nodes among immigrant; so security is naturally added into the routing protocol where nodes estimates trust levels of others on the basis of a set of attributes. Unlike the fixed possibilities of loosing data packets followed in previous routing techniques, novel proposed forwarding rule is implemented on the basis of the attribute similarity and gives a suggested method in evaluating the degree of similarity among attributes. The simulations show that the introduced pathing technique works better as compared to Dynamic Source Routing (DSR) protocol against the black hole attack and behavior altering attacks and that it is not affected by slander attacks. The effects of transportation range, velocity, and number of sensor nodes on pathing performances is also examined by authors.

Sink position secrecy is one of the big issues in Wireless Sensor Networks (WSNs) where attackers may find the sink by monitoring the destination of data packets, controlling and scaling the flow of data, which causes disclosure of the sink-position secrecy. In this paper [8], authors have proposed a Ring Based Routing (RBR) technique to focus on the problem of sink-position secrecy in WSNs. The RBR technique is consists of various routing rings and routing lines where the nodes data is not directly transmitted to the sink but to the closest routing ring. In this, data is transmitted via each sensor node in the ring and then transmitted to other routing rings via routing lines, where the number of ambiguity sink nodes is same as the total number of sensor nodes in the network. More precisely, under the RBR technique the routing rings move in random arrangements which can trouble attackers even if the sink position is static and this extremely enhances the sink-position secrecy. Also the routing rings are formed as per the exhaustive monitoring of network energy, which can entirely utilize the remaining energy and enhance energy efficiency and network lifespan. Both hypothetical analysis and simulation outcomes specify that proposed technique can protect position secrecy of sinks efficiently.

An attacked node can produce a bogus report, which appears in wrong alarms, data loss, and a desolation of valuable network energy. In this paper [9], authors have proposed interweaved hop-by-hop authentication (IHA) technique to reduce such genuine harm by finding and filtering wrong reports at the very initial en-route sensor nodes. Unluckily, hop-by-hop authentication (IHA), with a one route from the source to the base station, can't retain its security objective if more than t intervening nodes are compromised. Here authors have proposed an enhanced multi-path interleaved hop-by-hop authentication (MIHA) technique. MIHA forms dislocated and interweaved paths and transforms to replacement paths when there is more than t attacked nodes on the current route to continue negotiating with en-route insider attacks. A new key assignation scheme was also practiced to increase network security and to decrease key storage overhead. Through monitoring and simulations, MIHA shows enhanced resilience to en-route insider attacks and refines more fraudulent reports at initial hops than IHA.

In this paper [10], authors have designed and studied DoS attacks to determine the harm that crucial-to-find attackers can cause. The first attack which is studied by authors named the JellyFish attack is applied on the closed-loop flows like TCP; even though protocol obedient, it has destructive effects. The second type of attack is the Black Hole attack, which has consequence same as that of JellyFish, but on open-loop flows. Authors measure through simulations and examining the scalability of DoS attacks as a job of key performance attributes like mobility, size of system, node density, and counter-DoS approach. The result shows that such DoS attacks can enhance the capability of ad hoc networks, as they refrain multi-hop flows and only enable one-hop communication, a capacity-enhancing, still clearly unacceptable condition.

Table 1: Literature Survey

Sr. No.	Title	Author and year	Technique used	Advantages	Disadvantages
1.	ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks [1]	Yuxin Liu, Mianxiong Dong, Anfeng Liu (2016)	Authors have proposed active detection-based security and trust routing technique for wireless sensor network called as ActiveTrust. In this, numbers of detection routes are actively created to immediately detect and calculate nodes trust values in order to enhance the data packet route security.	Allows energy efficient, reliable and secure routing of data.	Trust evaluation and hence routing efficiency can be improved.
2.	An Efficient Countermeasure to the Selective Forwarding Attack in Wireless Sensor Networks [2]	Hung-Min Sun, Chien-Ming Chen, and Ying-Chu Hsiao (2007)	In this, MDT strategy is used which isolates the network into two dataflow topologies. Alike if one topology has a mischievous sensor node, the BS can still receive data packets via other topology.	The BS receives the information on time without resending it even some packets have been lost, Scheme is lightweight and simple.	The energy utilization will be *n* times that of a single path route, which will seriously affect the network lifetime.
3.	H-SPREAD: A	Wenjing Lou,	*H-SPREAD* integrates the path formation	Very efficient with less	H-SPREAD only improves

	Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks [3]	*Member, IEEE*, Younggoo Kwon, *Member, IEEE(2006)*	process and hybrid message transportation scheme. It holds the benefits of a *threshold secret sharing* and route diversification of multipath data promoting to boost path flexibility against node breakdown or compromise routes. Data packets can be protectively forwarded towards the sink node even when a short number of sensor nodes or routes have are attacked during the data transportation process.	than one message per path. Scheme is more resilient to node/link failures and a collusive attack of compromised nodes. Improves both reliability and security at the same time.	reliability and security of data delivery in the network, but it cannot enhance security of individual nodes.
4.	PHACK: An Efficient Scheme for Selective Forwarding Attack Detection in WSNs [4]	Anfeng Liu, Mianxiong Dong, Kaoru Ota and Jun Long (2015)	A Per-Hop Acknowledgement (PHACK)-based technique is introduced for every packet transposition to find selective forwarding attacks. Here, the BS and every sensor node along the prolonging path produce an (ACK) acknowledgement / feedback message for every obtained packet to certify the ordinary packet transmission.	High detection probability and the ability to identify suspect nodes, Easy to implement.	Protocol cannot work in crowd sensing networks to prevent selective forwarding attacks i.e. where the powerful adversary can collude with other attackers to launch attacks.
5.	Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes [5]	Tao Shu, Sisi Liu, and Marwan Krunz (2010)	In this algorithm estimates various paths in a arbitrary manner every time an information packet wish to be transmit, such that the set of paths taken by multiple shares of distinct packets keep altering over time. As an outcome, a more number of routes can be possibly produces for each source and target.	Routes generated by our mechanisms are also highly dispersive and energy-efficient as compared to previous techniques.	To generate the new route each time more energy is consumed and thus slightly reduces the lifespan of network.
6.	Toward Energy-Efficient Trust System through Watchdog Optimization for Wsns [6]	Peng Zhou, Siwei Jiang, Athirai Irissappane, Jie Zhang, Jianying Zhou, and Joseph Chee Ming Teo (2015)	Authors have proposed a series of escalation methods to reduce the energy expenditure of watchdog usage, while maintaining the system's security in a satisfactory level. Authors' donation subsists of hypothetical analyses and practicable algorithms, which can conveniently and effectively line up the watchdog job depending on the sensor nodes' position and the destination nodes' truthfulness.	Reduces the energy cost induced by watchdog tasks as much as possible, while keeping trust accuracy and robustness in a sufficient level.	Load balancing problem
7.	Building a trusted route in a mobile ad hoc network considering communication reliability and path length [7]	J. Wang, Y. H. Liu, Y. Jiao (2011)	Authors have proposed a new trusted path which considers communication reliability and route length for a reliable and feasible data packet delivery in a MANET. Attribute similarity concept is proposed in detecting possibly friendly sensor nodes among immigrant.	Provides communication reliability and allows feasible data packet delivery.	Extra overhead of evaluating the degree of similarity among attributes
8.	An energy-efficient and sink-location privacy enhanced scheme for WSNs through ring based routing	J. Long, A. Liu, M. Dong, et al. (2015)	Authors have proposed a RBR technique to focus on the issue of sink-position secrecy. Under the RBR technique the routing rings move in random arrangements which can trouble attackers even if the sink position is static and this extremely enhances the sink-position secrecy.	Proposed technique can protect position secrecy of sinks efficiently.	Overhead of maintaining routing rings and routing lines.
9.	A multi-path interleaved hop-by-hop en-route filtering scheme in wireless sensor networks	T. P. Nghiem, T. H. Cho (2010)	Authors have proposed MIHA scheme to reduce such genuine harm by finding and filtering wrong reports at the very initial en-route sensor nodes which forms dislocated and interweaved paths and transforms to replacement paths when there is more than t attacked nodes on the current route to continue negotiating with en-route insider attacks.	Gives enhanced resilience to en-route insider attacks and refines more fraudulent reports at initial hops	Replacement paths have to be maintained and used in case of more number of compromised no
10.	Impact of Denial-of-Service Attacks on Ad-Hoc Networks	I. Aad,P. J. Hubaux and W. E. Knightly (2008)	In this, two types of attacks named JellyFish attack and Black Hole attack are studied. JellyFish attack is applied on the closed-loop flows like TCP. Black Hole attack is applied on the open-loop flows.	The result shows that such DoS attacks can enhance the capability of ad hoc networks, as they refain multi-hop flows and only enable one-hop communication.	Works for only one hop in terms of communication. It can be improved to multihop communication.

3. Conclusion

WSNs have hugely extended in playing a key job for the data decisive selection and shipment. As the sensor nodes are deployed in neglected environment, they are more vulnerable to the attacks. If the attack is not detected in WSN, there is a chance of taking wrong decision and it is a serious issue in the sensitive fields such as in military, defense, etc. So there is a need to consider the issue of detecting and preventing such types of attacks and make the safe and reliable routing of data packets.

In this paper spotlight is on the studying various types of attacks that can be performed on the sensor node such as denial of service, Black hole attack, etc. Also the techniques to detect the sensor node under the control of adversary and the type of attack happened on the node are presented in the paper. It also includes a solution for secure and reliable routing of the data in WSN.

References

[1] Yuxin Liu, Mianxiong Dong, *Member, IEEE,* Kaoru Ota, *Member, IEEE,* Anfeng Liu, "ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks", IEEE Transactions on Information Forensics and Security, 1556-6013 (c) 2016

[2] H.Sun, C. Chen,Y. Hsiao, "An efficient countermeasure to the selective forwarding attack in wireless sensor networks," in Proc. Of IEEE TENCON 2007, pp. 1-4, 2007.

[3] W. Lou,Y.Kwon, "H-Spread: A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks," IEEE Transaction on vehicular technology, vol. 55, no. 4, pp. 1320-1330, 2006.

[4] A.Liu, M.Dong, K.Ota, et al."PHACK：An Efficient Scheme for Selective Forwarding Attack Detecting in WSNs," Sensors, vol. 15, no. 12, pp. 30942-30963, 2015.

[5] T. Shu, M. Krunz,S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," IEEE Transactions on Mobile Computing, vol. 9, no. 7, pp. 941-954, 2010.

[6] P. Zhou, S. Jiang, A. Irissappane, et al. "Toward Energy-Efficient Trust System Through Watchdog Optimization for WSNs," IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 613-625, 2015.

[7] J. Wang, Y. H. Liu, Y. Jiao, "Building a trusted route in a mobile ad hoc network considering communication reliability and path length," Journal of Network and Computer Applications, vol. 34, no. 4,pp. 1138-1149, 2011.

[8] J. Long, A. Liu, M. Dong, et al. "An energy-efficient and sink-location privacy enhanced scheme for WSNs through ring based routing," Journal of Parallel and Distributed Computing, vol. 81, pp. 47-65, 2015.

[9] T. P. Nghiem, T. H. Cho, "A multi-path interleaved hop-by-hop en-route filtering scheme in wireless sensor networks," Computer Communications, vol. 33, no. 10, pp. 1202-1209, 2010.

[10] I. Aad,P. J. Hubaux and W. E. Knightly, "Impact of Denial-of-Service Attacks on Ad-Hoc Networks," IEEE-ACM Transactions on Networking, vol. 16, no. 4, pp. 791-802, 2008.

[11] X. Liu, M. Dong, K. Ota, P. Hung, A. Liu. "Service Pricing Decision in Cyber-Physical Systems: Insights from Game Theory," IEEE Transactions on Services Computing, vol. 9, no. 2, pp. 186-198, 2016.

[12] S. J. Lee, M. Gerla, "Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Networks," IEEE ICC, pp. 3201-3205, 2011.

[13] Y. L. Yu, K. Q. Li, W. L. Zhou, P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," Journal of Network and Computer Applications, vol. 35, no. 3, pp. 867-880, 2012

Author Profile

Ms. Trupti Anil Bomble ,is currently pursuing M.E.(Computer) from Department of Computer Engineering, Jaywantrao Sawant College of Engineering, Pune, India. From Savitribai Phule Pune University, Pune , Maharashtra, India :411007.She received her B.E (Information Technology) Degree from Theem College of engineering, Boisar, Thane, Maharashtra 401501 from University of Mumbai. Her Area of Interest is Network Security and Wireless Sensor Networks.

Prof. M.D Ingle, is currently pursuing Ph.D. He received his M Tech. (Computer) Degree from Dr. Babasaheb Ambedkar Technological University Lonere, Dist. Raigad 402103 ,Maharashtra ,India. He received his B.E (Computer) Degree from Govt college of Engineering, Aurangabad, Maharashtra, India. He is currently working as M.E coordinator and Asso. Prof. (Computer) at Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India - 411007. His area of interest is network security and WSN.