http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 11 (1): 40-48, 2012
ISSN 1812-5638 / DOI: 10.3923/itj.2012.40.48
© 2012 Asian Network for Scientific Information

A Specification Based Intrusion Detection Mechanism for the LEACH Protocol

[1]Soojin Lee, [1]Yunho Lee and [2]Sang-Guun Yoo
[1]Department of Defense Information Science, Korea National Defense University, Seoul, Korea
[2]Department of Computer Science and Engineering, Sogang University, Seoul, Korea

Abstract: With the improvement of the wireless communication and embedded technology, the application of wireless sensor network has increased to various fields. However, such type of network embeds more vulnerabilities than others because of its resource constrained characteristic. To counteract such problem, traditional security mechanisms such as cryptography and authentication have been used. However, those are not enough to solve all security issues that may happen in the wireless sensor network, especially those attacks executed by a compromised node. This fact creates the need for a complementary security mechanism. This paper proposes a specification-based intrusion detection mechanism for the wireless sensor network, specifically for the popular cluster based Low Energy Adaptive Clustering Hierarchy (LEACH) protocol. It identifies the possible attacks in different phases of such protocol, develop the intrusion detection mechanism and execute simulations to analyze the efficiency of the proposed solution. This paper has also shown how the proposed mechanism offers a high intrusion detection rate while maintaining a low traffic overhead.

Key words: Wireless sensor network, low energy adaptive clustering hierarchy protocol, intrusion detection system, network simulation, misbehavior, security, network performance analysis

INTRODUCTION

The Wireless Sensor Network is a self-organized network system composed of low cost and resource limited sensor nodes. These type of networks has been widely used in applications such as habitat monitoring (Mainwaring *et al*., 2002), as an indoor sensor network (Carlson *et al*., 2003), for battlefield surveillance (UAF, 2010), for health monitoring (Otto *et al*., 2006) and others (Idris *et al*., 2009; Rozyyev *et al*., 2011; Chauhdary *et al*., 2009; Li *et al*., 2011). Even though this technology has been used widely, the sensor nodes do not include strong security mechanisms making them vulnerable from attacks. The vulnerabilities of the network increase if they are located in hostile environments without permanent management. Traditional security mechanisms such as encryption, access control and authentication have been used to address a part of the security problems of wireless networks. However, they have not been able to respond appropriately to every attack in the wireless network environment. Such limitations in sensor networks have created the need for additional security mechanisms, in order to maintain a high level of security (Khanafer *et al*., 2010; Mishra *et al*., 2004).

Intrusion detection techniques have been used in different areas (Raja *et al*., 2008; Yoo *et al*., 2011; Bahaman *et al*., 2011) and there are also many techniques, those can be classified into the categories of misuse detection, anomaly detection and specification based detection. Misuse detection (Porras and Kemmerer, 1992; Kumar and Spafford, 1994) which detects known misuses accurately, is not very effective against unknown attacks. Anomaly detection (Anderson *et al*., 1995; Forrest *et al*., 1997; Ghosh *et al*., 1999) handles unknown attacks better but can generate a lot of false positives and hence is not deployed widely. The specification-based approach (Ko *et al*., 1997; Sekar and Uppuluri, 1999) is similar to anomaly detection in the sense that it detects activities executed outside the boundaries of a normal pattern. However, it provides advantages such as the detection of novel attacks and the maintenance of a low degree of false alarms. Tseng *et al*. (2003) present a specification-based intrusion detection system for the Ad hoc On-demand Distance Vector (AODV) protocol was proposed which detects intrusion by using a finite state machine of the normal operational process. On the other hand, Gill *et al*. (2006) proposed a specification-based intrusion detection system for the IEEE 802.11 wireless network protocol to detect attacks and apply security policies. The last mentioned approach uses the specification of a state transition model of the network protocol and policy restrictions.

This study has proposed a specification-based intrusion detection mechanism suitable for wireless

Corresponding Author: Yunho Lee, Korea National Defense University, Seoul, Korea Tel: +82-10-5076-7673

sensor network routing protocols, specifically, for the popular LEACH (Low-Energy Adaptive Clustering Hierarchy) protocol. This paper analyzed the LEACH protocol to discover its vulnerabilities and identify possible misbehaviors and then proposed a specification-based intrusion detection mechanism for those vulnerabilities. The intention of this study was to propose an intrusion detection system for sensor networks as a complementary security mechanism.

BACKGROUND

Low Energy Adaptive Clustering Hierarchy (LEACH): Low Energy Adaptive Clustering Hierarchy (LEACH) (Heinzelman *et al.*, 2000) is a cluster-based routing protocol for a wireless sensor network which divides the network into small areas called clusters. In each cluster, a dedicated node called a Cluster Header (CH) is selected. The CH has the responsibility for creating and manipulating a TDMA (Time division multiple access) schedule. The CHs also has the responsibility to aggregate and send the data collected from other nodes of the cluster (member nodes) to the base station. The LEACH protocol is divided into rounds and each round consists of two phases: the set-up and steady phases (Fig. 1).

Setup phase: Each node decides independently if it will become a CH or not. This election probability is based on the last time a node has been elected as a CH. The node that hasn't been a CH for long time is more likely to elect itself than other nodes that have been CHs recently.

In the setup phase, each CH inform their neighbor nodes with an advertisement message that it has become CH. Non-CH nodes choose the advertisement message with the strongest received signal strength. The member nodes then inform to the chosen CH that they have become a member of that cluster using a "join message" which contains their identifications. After this phase, the each CH knows the number of member nodes and their identifications (Fig. 2). Based on the number of member nodes of the cluster, the each CH creates a TDMA schedule and broadcasts it to its cluster members.

Steady-state phase: This phase is started after the setup phase. In this phase, the data transmission is started. Member nodes send their data during their allocated Time Division Multiple Access (TDMA) slot to the CH. This transmission uses a minimal amount of energy which is only that required to reach the CH (calculated using the received strength of the CH advertisement). When all the data has been received, the CH aggregates these data and transmits it to the base station. LEACH can perform local aggregation of the received data in each cluster to reduce the amount of data that is transmitted to the base station.

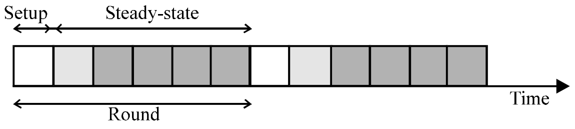

Fig. 1: LEACH Protocol Phases

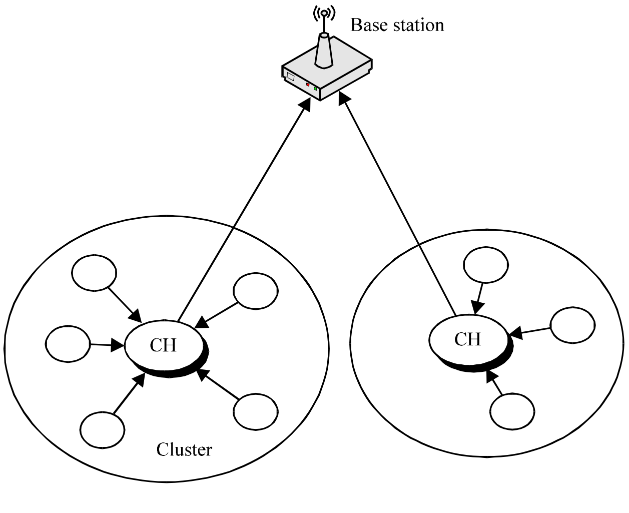

Fig. 2: LEACH Protocol Clustering

ENHANCED INTRUSION DETECTION SYSTEM FOR LEACH

Most sensor network security research has been centered in traditional mechanisms based on cryptography and research about LEACH has not been the exception. Security research about LEACH is focused on constructing secure communication channels using cryptographic techniques (Oliveira *et al*., 2006; Banerjee *et al*., 2007). However, these methods do not offer any protection if a valid node with authentic cryptographic keys is captured by the attacker and modified to execute misbehaviors. Therefore, appropriate security mechanisms additional to the traditional cryptographic method are required to determine such misbehaviors. This is the reason why this study proposed a specification-based intrusion detection mechanism as an additional security mechanism for the wireless sensor network environment.

Identification of misbehaviors: The LEACH protocol is divided into two major phases: the set-up and steady phases. However, such phases have been divided into four smaller phases to identify easily possible misbehaviors.

Advertisement phase: In this phase, each node determines whether it will become the Cluster Header (CH) or not and advertises the decision to other nodes of the cluster. In the LEACH protocol, CHs have a greater impact on the network than the ordinary nodes because they are responsible for collecting information from member nodes. For this reason, if a malicious node becomes a CH, the effect of the attack can be serious. In particular, if the malicious node maintains the condition of CH for long period of time, the effect of the attacks can be maximized. There are two possible misbehaviors in this phase of the protocol. First, the malicious node can become a CH continuously, taking advantage of the self CH election characteristic of the LEACH protocol. Second, the malicious node can transmit a strong signal to advertise itself as CH. The intention of the last one is to cover a wider cluster range making ordinary nodes to believe that it is the nearest node.

Cluster set-up: In this phase, an ordinary node selects the nearest CH and sends a join message to become a member of its cluster. The misbehavior that a malicious node can execute in this phase is to avoid the transmission of the join message to join a cluster. This misbehavior results in the omission of transmission of the data sensed by the node.

Schedule creation: This phase is executed after the CH receives the join message from the member nodes. In this phase, the CH sends the TDMA schedule to its member nodes. The misbehavior that could happen in this phase is that the CH omits the transmission of the TDMA schedule to the member nodes. With this attack, the member nodes are not able to transmit their sensed data to the base station.

Steady-state phase: In this phase, the CHs collect the information transmitted by the member nodes and forward it to the base station. There are two possible misbehaviors that a member node can execute in this phase. First, the malicious member node can omit the transmission of the sensed data. Second, the malicious node can intentionally transmit data in a time slot that belongs to another node to provoke collision and interfere with normal data transmission. The first attack makes impossible the collection of data from the region sensed by the affected node. The second attack blocks the collection of data even from non-affected nodes. On the other hand, if the malicious node were a CH, the attacker could forward the data to another destination, avoid the transmission of data collection to the base station or transmit false information to the base station.

Misbehavior subject to detection: In some cases, it is hard to distinguish if the misbehavior occurred because the node had become malicious or because the energy of the node has been depleted. For this reason, we have decided not to follow the misbehavior of each node but instead, to establish a misbehavior threshold for the network and block the misbehaviors when reaching such threshold. We have decided to omit the misbehavior related to the transmission of false information because this can be controlled using previous approaches, such as Wagner (2004), Yang *et al*. (2006) and Buttyan *et al*. (2006). The list of misbehaviors subject to control by the proposed specification-based intrusion detection mechanism is summarized in Table 1.

Intrusion detection architecture suitable for LEACH protocol: The architecture of our approach is based mainly on the distributed and cooperative intrusion detection architecture proposed by Zhang and Lee (2003) to detect misbehaviors. However, to enhance the lifetime of the sensor nodes, we use the powerful energy and performance capacity feature of the base station.

Figure 3 illustrates the architecture of the proposed intrusion detection mechanism. Each misbehavior detected by the nodes, including both the CHs and member nodes, are transmitted to the base station. The

Table 1: List of misbehaviors

Phase	Misbehavior	Effect
Advertisement	Continuous Header Election	Continuous attack as Cluster Header is possible
	Transmission of a Strong Signal	-Maximization of the attack effect by including as many nodes as possible in the cluster -Promote energy consumption by using long-distance data transmission
Schedule Creation	No transmission of TDMA schedule	Interfere with normal data transmission from member nodes
	TDMA Schedule Disobedience	Interfere the transmission/reception of sensed data
Steady- State	No transmission of Member Node's data	Omission of the local surveillance data
	No transmission of Header's data	Drop of all data sensed by nodes of a cluster

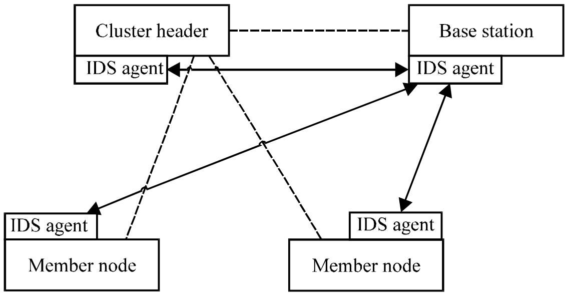

Fig. 3: Structure of the proposed intrusion detection technique

base station, then analyzes the collected data to decide the response action to take.

This structure reduces the workload of the nodes by delegating to the base station the processes related to the analysis of data related to misbehaviors. The task is delegated to the base station because it has a much better energy and performance capacity. This structure allows nodes to have longer lifetimes and be more trustworthy because all calculations are executed by the trusted base station.

Misbehavior detection: The misbehaviors subject to identification by the proposed intrusion detection system are six. The details of how they can be detected are explained in this subsection.

Continuous header election: Continuous cluster header election can be detected easily by comparing the current CH identification with the elected CH identification. Here, the proposed mechanism assumed that the malicious nodes cannot falsify the nodes' identifications because they are protected using cryptographic solutions. This process can be implemented by using a small storage memory of nodes. Each node stores in its memory the identification of the elected CH and in each new setup phase, the new CH identification is compared with the previous one. If the number of comparisons that are true is greater than the threshold value, it is notified as misbehavior.

Transmission of a strong signal: To identify the strong signal transmission misbehavior, it is necessary to verify if the sending node is really near the receptor nodes. To verify the real position of the CH candidate, the ordinary nodes must calculate the distance to the candidate node using the strength of the signal. The ordinary nodes send the join message with equal signal strength in order to reach the destination. Then, only if a TDMA schedule comes back, the candidate is selected as the node's CH. Otherwise, if there is not a response, the node concludes that the candidate has sent a strong signal and identifies this as misbehavior (Fig. 4).

No transmission of the TDMA schedule: If the ordinary node transmits the join message to the CH and does not receive a response from it in a predefined period of time, this case is considered as misbehavior.

TDMA schedule disobedience: This misbehavior is easily recognized by comparing the identification of the node sending the message with the identification in TDMA schedule. If a node sends a data message in a different time slot than that allocated for it, this activity is identified as misbehavior.

No transmission of member Node's data: The CH distinguishes it as misbehavior when a member node does not transmit any data in its time slot in the TDMA schedule. This is recognizable because the cluster header has the information about the TDMA schedule.

No transmission of header's data: When the CH sends data, the surrounding member nodes can listen to the message. Therefore, if the member nodes do not detect any message from the CH until their next transmission time slot, it is recognized as misbehavior.

Extended LEACH protocol specification for misbehavior detection: The condition to make a transition from one phase to another is very simple in the LEACH protocol. Therefore, we have considered that it is adequate to create a state transition diagram of the LEACH protocol and then add the intrusion detection states to such a diagram.

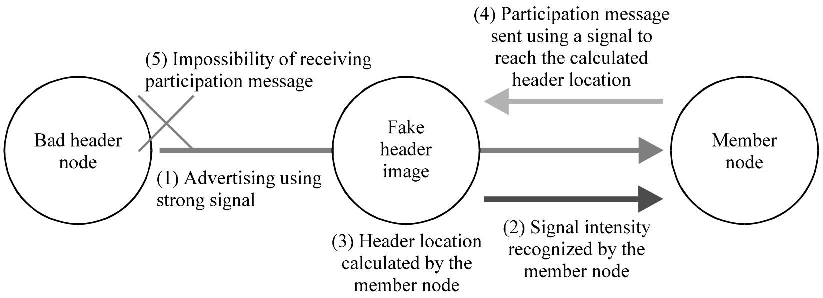
(4) Participation message sent using a signal to reach the calculated header location
(5) Impossibility of receiving participation message
Bad header node
Fake header image
Member node
(1) Advertising using strong signal
(3) Header location calculated by the member node
(2) Signal intensity recognized by the member node

Fig. 4: Strong signal misbehavior detection method

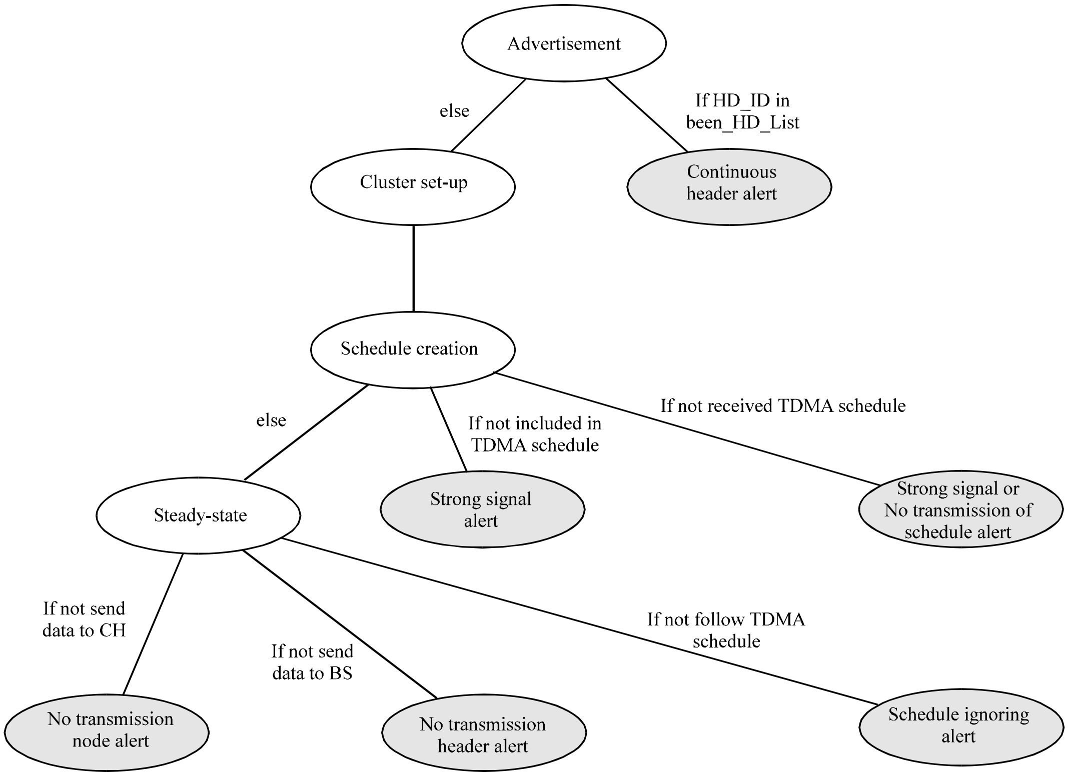

Fig. 5: State Transition Diagram of Extended LEACH Protocol Specification

Figure 5 illustrates the state transition diagram of the LEACH protocol extended with the misbehavior detection specification. This diagram differentiates the normal states of the LEACH protocol to the states of misbehavior detections.

SIMULATION AND ANALYSIS

Simulation environment: We have implemented the simulation environment using NS-2 which is widely used for network simulation (Viswacheda *et al*., 2007; Liao *et al*., 2005; Wang *et al*., 2011). The network area was 100×100 m containing 100 sensor nodes and one base station. Cluster headers were elected every 20 periods and the number of CHs was set to 5% of the total number of sensor nodes in the network. To provide a simulation environment similar to reality, we have introduced around a 0.3% traffic error rate. Malicious nodes performing random attacks were selected randomly among the 100 nodes. The numbers of malicious nodes were 5, 10 or 30% depending on the simulation.

Performance analysis: Figure 6 shows the message transmission rate of the LEACH protocol before and after implementing the intrusion detection mechanism when no attacks are being executed. The simulation shows how the

Table 2: Message transmission overhead caused by the intrusion detection system

Round	No. of alert messages	No. of attacks handled	No. of additional packets	Total No. of normal packets	Packet increase rate (%)
1	374	6	974	121000	0.8
2	250	6	580		0.7
3	298	2	498		0.4
4	285	1	385		0.3
5	441	10	1441		1.2
6	593	5	1093		0.9
7	274	0	274		0.2
8	492	5	992		0.8
9	370	3	670		0.5
10	291	3	591		0.5
11	569	9	1469		1.2
12	526	4	926		0.8
13	348	5	848		0.7
14	443	3	743		0.6
15	181	0	181		0.2
16	239	4	639		0.5
17	385	3	685		0.6
18	308	6	908		0.8
19	363	1	463		0.4
20	209	2	409		0.3

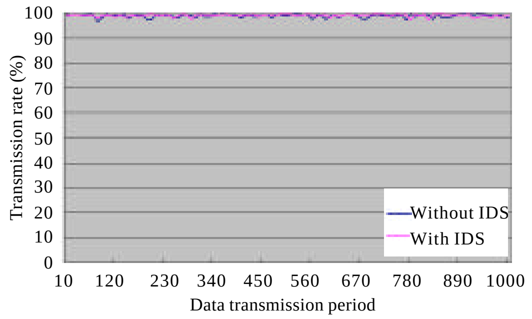

Fig. 6: Transmission rate comparison before and after implementing the intrusion detection system (without attack)

proposed solution does not generate any considerable negative effect over the network performance.

Table 2 details the message transmission overhead generated by the intrusion detection mechanism. It shows an increase of 0.2~1.2% additional messages. We believe that this overhead is acceptable compared with cryptography based solutions such SecLEACH which generates around a 20% overhead.

On the other hand, Table 3 illustrates the intrusion detection rate of the mechanism. It shows how the proposed mechanism provides a high performance in detecting misbehaviors, over 90% in every case.

The misdetection of misbehaviors 2, 3 and 6 is caused when the cluster header does not have any member node or their number is low and there is error in transmitting messages or when the alert message is lost during its transmission to the base station because of a network error.

Table 3: Detection rate of misbehaviors

Misbehavior	Detection rate (%)
Continuous header election	100
Transmission of strong signal	93
No transmission of schedule	94
TDMA schedule disobedience	99.9
No transmission of member node's data	98.85
No transmission of header's data	99.9

On the other hand, the misdetection of misbehaviors 4 and 5 is caused by errors of transmission of the join message sent by the member nodes to their CHs or misbehavior alert messages sent to the base station.

The analysis of the previous simulation shows how the proposed mechanism provides high rates of intrusion detection while maintaining a low performance overhead. Therefore, we expect that the mechanism will provide an effective complementary security mechanism without a considerable degradation of network performance.

Result of detection of attacks: The simulation included the execution of three different types of attack scenarios to verify the improvement of the network performance when the proposed mechanism detects the misbehaviors of malicious nodes.

The threshold for sending alarm messages was set to 2~3 of the same misbehavior detections. This threshold is not an optimized value. The value of the threshold requires to be configured depending on the reliability of the network condition of the real environment. It is important to remind that a low threshold can reduce the attack lifetime but with the understanding that it can also lead to false positives.

Attack scenario 1: In this scenario, the malicious node elects itself as a cluster header continuously by sending

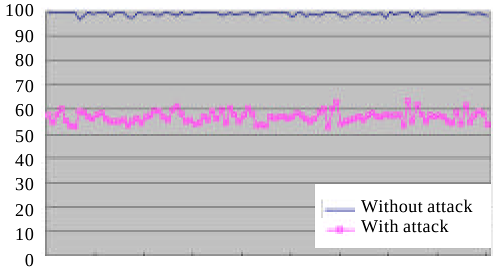

Fig. 7: Attack 1 simulation result without intrusion detection technique

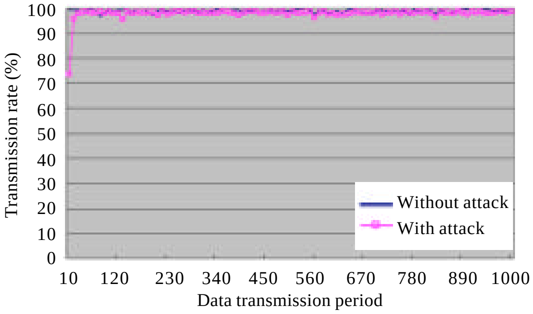

Fig. 8: Attack 1 simulation result after intrusion detection technique

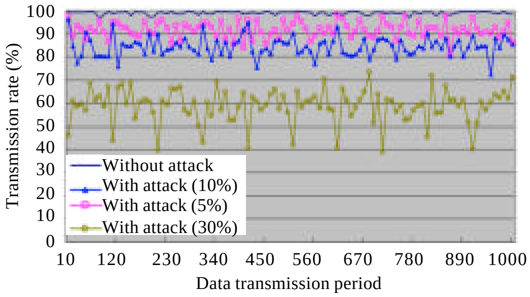

Fig. 9: Attack 2 simulation result without intrusion detection technique

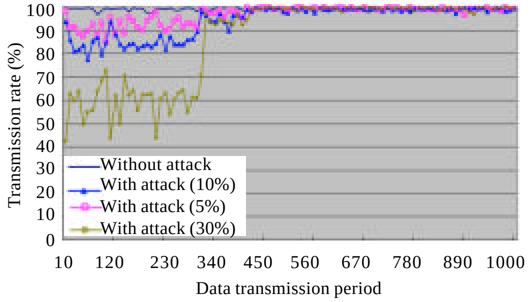

Fig. 10: Attack 2 simulation result after intrusion detection technique

a strong signal. Once the cluster is setup, it drops the data messages received from member nodes.

The data transmission rate variation of the attack is shown in Fig. 7. It shows how the correct transmission rate is affected considerably. The affected data rate will depend on the size of the malicious cluster; the bigger the cluster the bigger the data loss. This type is considered to be one of the most catastrophic attacks.

Figure 8 shows the change in the network performance after the implementation of the intrusion detection mechanism. It shows how the data transmission is degraded at the beginning but after the misbehavior detection and the isolation of malicious nodes, the data transmission recovers to the normal level. Figure 8 summarizes how the proposed mechanism can neutralize this attack.

Attack scenario 2: In this attack, the malicious node becomes a cluster header by using a strong signal but it does not transmit the TDMA schedule to member nodes. This attack has as its goal the isolation of member nodes from the network.

Figure 9 shows the transmission rate with 5, 10 and 30% malicious nodes. It illustrates how the number of malicious nodes is directly proportional to the degradation of the correct transmission rate.

On the other hand, Fig. 10 illustrates the same network condition of Fig. 9 but with the proposed intrusion detection mechanism. The proposed solution recovers considerably the data transmission rate by isolating the malicious nodes. The loss of data packets at the beginning of the attack is caused while the misbehavior threshold is in the process of being reached.

Attack scenario 3: In this attack, the malicious node announces itself as CH using the normal signal strength. Once it receives the data messages from the member nodes, it omits their forwarding to the base station.

Figure 11 shows a similar phenomenon to attack scenario 2 but with a higher data transmission rate. This means that attack scenario 2 has a more negative impact than this one. The reason for this effect is that the malicious node creates a larger cluster by using a strong signal in the attack in scenario 2.

Figure 12 illustrates the performance of the network with the intrusion detection mechanism. It shows how the performance of the network recovers faster than the previous one. This is because attack scenario 2 is

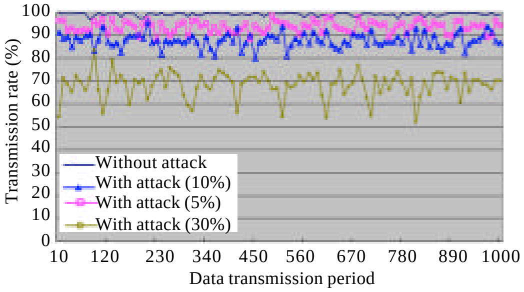

Fig. 11: Attack 3 simulation result without intrusion detection technique

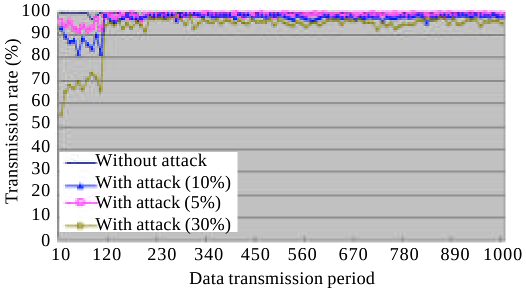

Fig. 12: Attack 3 simulation result after intrusion detection technique

executed in the cluster setup phase, while scenario 3 is executed in the data transmission phase which gives a longer period of time allowing the number of misbehaviors to reach the threshold faster and consequently isolating the malicious nodes faster as well.

CONCLUSION

This study proposes a specification-based intrusion detection mechanism suitable for the LEACH protocol. First the possible misbehaviors in each phase of the protocol were identified. Then, the misbehaviors to be controlled by the proposed algorithm were selected. The paper also has defined an extended specification of the normal and abnormal flow of the LEACH protocol to implement, based on this flow, the proposed security mechanism. The simulation has shown that the proposed mechanism offers a high intrusion detection rate while maintaining a low traffic overhead. It has also demonstrated that it is suitable for the LEACH protocol. This work expects that the specification based intrusion detection mechanism proposed in this paper will be useful as a complementary security solution for sensor networks implemented in a hostile environment.

REFERENCES

Anderson, D., T. Lunt, H. Javitz, A. Tamaru and A. Valdes, 1995. Next-generation intrusion detection expert system (NIDES): A summary. SRI-CSL-95-07, SRI International.

Bahaman, N., A.S. Prabuwono and M.Z. Masud, 2011. Implementation of IPv6 network testbed: Intrusion detection system on transition mechanism. J. Applied Sci., 11: 118-124.

Banerjee, P., D. Jacobson and S.N. Lahiri, 2007. Security and performance analysis of a secure clustering protocol for sensor networks. Proceedings of the 6th IEEE International Symposium on Network Computing and Applications, July 12-14, 2007, IEEE, pp: 145-152.

Buttyan, L., P. Schaffer and I. Vajda, 2006. RANBAR: RANSAC-based resilient aggregation in sensor networks. Proceedings of the 4th ACM Workshop on Security of Ad-Hoc and Sensor Networks, (SAAN'06), ACM., pp: 83-90.

Carlson J., R. Han, S. Lao, C. Narayan and S. Ghani, 2003. Rapid prototyping of mobile input devices using wireless sensor nodes. Proceedingsof the 1st IEEE Workshop on Mobile Computing Systems and Applications, October 9-10, 2003, USA., pp: 21-29.

Chauhdary, S.H., A.K. Bashir, S.C. Shah and M.S. Park, 2009. EOATR: Energy efficient object tracking by auto adjusting transmission range in wireless sensor network. J. Applied Sci., 9: 4247-4252.

Forrest, S., S.A. Hofmeyr and A. Somayaji, 1997. Computer immunology. Comm. ACM., 40: 88-96.

Ghosh, A.K., A. Schwartzbard and M. Schatz, 1999. Learning program behavior profiles for intrusion detection. Proceedings of the 1st USENIX Workshop on Intrusion Detection and Network Monitoring, April 9-12, 1999, USA., pp: 51-62.

Gill, R., J. Smith and A. Clark, 2006. Specification-based intrusion detection in WLANs. Proceedings of the 22nd Annual Computer Security Application Conference, December 2006, USA., pp: 141-152.

Heinzelman, W.R., A. Chandrakasan and H. Balakrishnan, 2000. Energy-efficient communication protocol for wireless microsensor networks. Proceedings of the 33rd Hawaii International Conference on System Sciences, January 4-7, 2000, Washington, DC., USA. pp: 8020-8020.

Idris, M.Y.I., E.M. Tamil, N.M. Noor, Z. Razak and K.W. Fong, 2009. Parking guidance system utilizing wireless sensor network and ultrasonic sensor. Inform. Technol. J., 8: 138-146.

Khanafer, M., M. Guennoun and H.T. Mouftah, 2010. Intrusion detection system for WSN-based intelligent transportation systems. Proceeding of the IEEE Globecom, December 6-10, 2010, IEEE, pp: 1-6.

Ko, C., M. Ruschitzka and K. Levitt, 1997. Execution monitoring of security-critical programs in distributed systems: A specification-based approach. Proceedings of the IEEE Symposium on Security and Privacy, May 4-7, 1997, IEEE Computer Society Washington, DC, USA.

Kumar, S. and E. Spafford, 1994. A pattern-matching model for intrusion detection. Proceeding of the 17th National Computer Security Conference, October 1994, Baltimore, pp: 11-21.

Li, Z., R. Li, T. Pei, Z. Xiao and X. Chen, 2011. Survey of geographical routing in multimedia wireless sensor networks. Inform. Technol. J., 10: 11-15.

Liao, H.C., Y.W. Ting, C.M. Chen and C.C. Yang, 2005. A performance comparison of Ad hoc routing protocols based on ant mobility model. Inform. Technol. J., 4: 278-283.

Mainwaring, A., J. Polastre, R. Szewczyk, D. Culler and J. Anderson, 2002. Wireless sensor networks for habitat monitoring. Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications, September 28, 2002, ACM New York, USA., pp: 88-97.

Mishra, A., K. Nadkarni and A. Patcha, 2004. Intrusion detection in wireless ad hoc networks. IEEE Wireless Communicat., 11: 48-60.

Oliveira, L.B., H.C. Wong, M. Bern, R. Dahab and A.A.F. Loureiro, 2006. SecLEACH-A random key distribution solution for securing clustered sensor networks. Proceedings of the 5th IEEE International Symposium on Network Computing and Applications, July 24-26, 2006, Cambridge, MA., pp:145-145.

Otto, C., A. Milenkovic, C. Sanders and E. Jovanov, 2006. System architecture of a wireless body area sensor network for ubiquitous health monitoring. J. Mob. Multimed., 1: 307-326.

Porras, P.A. and R.A. Kemmerer, 1992. Penetration state transition analysis: A rule based intrusion detection approach. Proceedings of the 8th Annual Computer Security Applications Conference, November 30-December 4, 1992, USA., pp: 220-229.

Raja, P.C.K., M. Suganthi and R. Sunder, 2008. Wireless node misbehavior detection using genetic algorithm. Inform. Technol. J., 7: 143-148.

Rozyyev, A., H. Hasbullah and F. Subhan, 2011. Indoor child tracking in wireless sensor network using fuzzy logic technique. Res. J. Inform. Technol., 3: 81-92.

Sekar R. and P. Uppuluri, 1999. Synthesizing fast intrusion prevention/detection systems from high-level specifications. Proceedings of the 8th Conference on USENIX Security Symposium, August 23-36, 1999 Washington, D.C., USA., pp: 63-78.

Tseng, C.Y., C. Ko, R. Limprasittiporn, J. Rowe and K. Levitt, 2003. A specification-based intrusion detection system for AODV. Proceedings of the 1st ACM Workshop on Security of ad-hoc and Sensor Networks, October 27-30, 2003, USA., pp: 125-134.

UAF, 2010. ARGUS advanced remote ground unattended sensor systems. Department of Defense.

Viswacheda, D.V., L. Barukang, M.Y. Hamid and M.S. Arifianto, 2007. Performance evaluation of mobile ad hoc network based communications for future mobile tele-emergency system. J. Applied Sci., 7: 2111-2119.

Wagner, D., 2004. Resilient aggregation sensor networks. Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, October 25, 2004, ACM New York, pp: 78-87.

Wang, W., Z. Liu, X. Hu, B. Wang, L. Guo, W. Xiong and C. Gao, 2011. CEDCAP: Cluster-based energy-efficient data collecting and aggregation protocol for WSNs. Res. J. Inform. Technol., 3: 93-103.

Yang, Y., X. Wang, S. Zhu and G. Cao, 2006. Sdap: A secure hop-by-hop data aggregation protocol for sensor networks. ACM Trans. Inform. Syst. Security, 11: 356-367.

Yoo, S.G., S. Lee, Y. Lee, Y.K. Yang and J. Kim, 2011. Enhanced intrusion detection system for PKMv2 EAP-AKA used in WiBro. Inform. Technol. J., 10: 1882-1895.

Zhang, Y. and W. Lee, 2003. Intrusion detection techniques for mogile ad hoc networks. ACM WINET J., 2003: 1-16.