The Introduction of a Covert Channel in Hidden Transportation for Integrity Protocol in Wireless Sensor Networks

Riaz ullah Khan
University of Sunderland, UK

Abstract– **At the end of 20th century and at the beginning of 21st century Wireless Sensor Networks are widely exercise for the military purposes, industrial purposes as well as for educational purposes. Still Sensors are not yet exercised according to its potential. In these situations the network operator will observe Integrity of the network components, and as a result the problem of trusting the whole system will arise, weather to trust the entire system or not .The issue is that we require a safe, Secure and protected channel among the devices and components for every Integrity protocol. As a result we will propose a Covert channel for hidden transportation of Integrity monitoring messages and this Covert channel will make us able to hide Integrity check messages entrenched within the normal traffic without offering to a malicious node a chance to exercised an Integrity protocol.**

Keywords– **Wireless Sensor Networks, Integrity Protocol and Covert Channel**

I. INTRODUCTION

A Wireless Sensor Networks (WSN) Consists of spatially disseminated independent Sensors to check Environments, like movements, pressure, humidity, and sound etc to transmit their Information throughout the Network to the most important position cooperatively [1].

The further Up to date Networks are bi-directional, as well as to capable the control of the Sensor movement. The progress of Wireless Sensor Networks was provoked by armed forces purposes for example. Battleground observation; nowadays Such Networks are executed in many industrial and end User purposes, like industrial procedure observe and control etc. The Wireless Sensor is made by the network nodes from few hundred to many thousands of nodes where each and every node will be connected to one or sometime to many Sensors .each and every Sensor Network Node has normally numerous sections.

A Sensor Node may differ in volume from the shoebox to the size of the grain of the dust, The price of Sensor Nodes is likewise changeable; depend on the complication of the single Sensor Nodes. size and price restrictions on Sensor Nodes effect in resultant restrictions on assets like energy, computational rapidity, energy and bandwidth. The topology of the Wireless Sensor Networks be able to differ from a simple star Network to a sophisticated multiple hop Wireless mesh Network. The hops of the network know how to be flooding or routing [2], [3] with the help of propagation technique.

In the field of telecommunication and networking, Wireless Sensor Networks are an energetic research spot by means of a variety of workshop and conferences approved every year. The considerable advancement of Hardware industrialized Technology and Efficient Software Algorithms formulate a Network consist of a range of, undersized, low-priced Sensors, by technique of Wireless Communication. A Wireless Sensor Networks (WSN) [1]–[3] is a capable Network Infrastructure for various Applications like Environmental observe medical concern, and domestic device managing. This is mainly proper for battlefield observation and homeland safety situations Safety measures means are necessary to defend Wireless Sensor Networks from malevolent hits. So the safety measures in Wireless Sensor Networks turn out to be a vital and demanding plan charge.

Wireless Sensor Networks (WSNs) have been exercised for various Applications as well as military observation, capability monitor, and Environmental monitoring. Usually, WSNs have a huge amount of Sensor Nodes with the capability to correspond among them and also to an exterior Sink or a base-station [4], [5]. The Sensor from time to time detects the Data, practice it, and Pass on it to the Base Station. The frequency of Data exposure and the Number of Sensors, which details Data usually, relies on the precise Application. A detailed Survey on Wireless Sensor Networks is showed in [6]. Beside from safe, Secure and a protected channel Communication channel, the important apprehension in Wireless Sensor Networks is the Integrity of Nodes.

Integrity of Nodes exercises a trusted platform module confirmed by an attestation protocol, to attest the Integrity of cluster head [7]. To facilitate a Wireless Sensor Networks operator to reply to corrupt effort, data concerning node Integrity need to be substituted all through the network .If such Information is substituted clearly, attacker possibly conscious of the truth that the network is being monitored. Examination of replaced Information may still expose how frequently such Information is replaced and if no suitable Cryptographic actions are taken, it may also be probable to inform what Information is replaced.

As an explanation, the Integrity monitoring information might be covertly surrounded into traffic that fits the recognized explanation of the Wireless Sensor Networks, for example. To measure the temperature of the environment it

will avert Attackers from decisive what Information is replaced in order to evaluate node Integrity, but it will be impossible to tell whether the Integrity of a specific network is in reality being monitored. Plain encryption of the Communication channel in features does not offer an analogous level of deception.

II. REQUIREMENTS

As according to [8], the "quality of the covert channel can be articulated in expressions of detect ability in differentiate ableness (hidden Data cannot be alienated from the cover Information) and bandwidth i.e., hidden data to cover data"; yet, a covert channel for Integrity monitoring not only be of adequate superiority in term of this explanation as well as fulfill some specific needs resultant from examination situations.

1) Delay: in general, Covert channels have a corresponding small proportion of hidden Data to Cover Data. Additionally, they depend on the incident of network traffic that can be exercised to Cover Up for the hidden Communication. But to offer the way for competent organizational response, a practical utmost wait for occasion notification is necessary. In case of Covert channels, signaling a decisive system occurrence could depend on usual Cover traffic scheduled.

Regarding situations for example monitoring decisive infrastructure or even in military situations, unbroken and adequate network traffic are unspecified.

2). Recurrence: If a Covert channel is exercised to continually exchanging information probably unaffected Information of a node. The test is as a result not only to cover irregular, conflicting incident announcements but as well to mask the Communication of frequent actions or health Information.

3) One way(unidirectional) channel: For the reason of this arguments simply a One way(unidirectional) channel is essential, still if Wireless Sensor Networks in examination and military situations would promote from a bidirectional Communication channel for transmitting Sensor control commands. It's because that the simplicity spotlights of this Paper is lessened and the consequences from a One way(unidirectional) Communication channel can probably be transmitted to a bidirectional these situations.

III. RELATED WORK

Covert channels were initially explains by Lampson as channels "not planned for Information transmitting at every similar service programs cause on the system load" [3]. Covert channels can be categorized in the broad area of Information hiding. On the other hand, there is no obvious separation among stegnography and Covert channels. A probable justification is that Covert channels ascertain Information moves among entities which On the other hand not be allowable to exchanging information at all or with channels that are not proposed for Communication, while stegnography allows entities to exchanging information supplementary Information between valid data. The word "Covert channels" appears to have succeeded in the perspective of Networks and is exercised to explain any Information hiding advances in Network Communications, at times may be mixed with "stegnography".

Simmons *et al*. [4] introduced a descriptive, however proper setting for the stegnographic dilemma: Two prisoners (for example, Alice and Bob) are only allowable to exchanging information with a warden (for example, Willie). Their objective is to plan a break out plan with not the warden detecting as the warden expects to misinform them by changing Communication or launching false messages [5].

As there are two kinds of Covert channels can be eminent by their understanding [6]. Storage-based Covert channels engage the direct or indirect reading and writing of storage sPa ce location among dissimilar processes. Actually, Covert channels can also be distinguished by the layer(s) of the OSI reference model on which they function. Handel and Sandford [2] verified how each OSI layer might be exercised as a foundation for executing a Covert channel.

The assessment of Covert channels is only achievable with view to a precise operation. yet at this Point, it is understood that protocol header exploitation will distribute improved routine than Payload stegnography. At the same time, a protocol header exploitation algorithm for a Communication protocol introduces fewer necessities on the specific type of Cover traffic evaluated to applying stegnography to the Cover Payload. Therefore, this Part is focused on Covert channels based on Network header management.

IV. DESIGN OF A NETWORK COVERT CHANNEL FOR INTEGRITY MONITORING (NCCIM)

This part of the paper enlarge a design of a one way (unidirectional) channel that unite a sensor agent application and monitoring application, which operate successively on dissimilar network nodes. This model of a network covert channel for Integrity Monitoring (NCCIM) is planned to be a modular framework for given that vigorous communication among Sensor and monitor. The framework is depending on the OSI reference model to offer elasticity for execution.

The conveyance stacks of the Network Covert Channel for Integrity monitoring is dependable for inserting the Covert traffic on a node that is monitored by a sensor agent. It connects with the sensor agent application and the Cover traffic source, which is the subsystem managing network traffic produced by other services operate successively on that node. Analogously, the Network Covert Channel for Integrity monitoring receiving stack extracts the Covert monitoring Information on the node running successively the monitoring application. It connects with the Cover traffic sink, which is the subsystem conscientious for getting network traffic of that node, and the monitoring application. The Network Covert Channel for Integrity monitoring model provides a framework for the adjustment and interception of Cover traffic .monitoring Information is covertly exchanging information from Sensors to a monitor. The Covert channel is developed given the subsequent suppositions concerning the Nodes successively the Sensor agent or monitoring agent:

1) The overt services running successively on the node being monitored produce an uninterrupted traffic flow that offers an Upper bound on the Delay of the Covert channel.

2) The subsystem of the Nodes dependable for transmitting network traffic (traffic source) and the subsystem conscientious of getting network traffic (traffic sink) permit traffic to be adapted and to be interrupted, correspondingly.

3) The Nodes running successively the Sensor agents are depend on an implementation model that allows concurrency.

4) Each Sensor agent informs to the same monitor.

NCCIM is not conscientious for congregation monitoring data, which is executed by the Sensor agents, or examining such Data, which is the job of the monitoring agent. On the other hand, the Covert channel has to make sure some agent, and monitoring agents should be administered by the NCCIM. As normal Communication responsibilities from transport to physical layer require to be completed. Therefore, the Network Covert Channel for Integrity monitoring have to function on OSI layers 1 (Physical layer) to6 (Session layer).monitoring Information grouped by the Sensor agents can be shown in a variety of arrangements. Well-known standard arrangements contain SYSLOG messages or the RMON MIB. Conventional plan may be depending on XML, but it is also likely to use an optimized binary format. The definite demonstration of the monitoring Information is consequently out of the range of this architecture. On the other hand, it is appropriate if all messages are of permanent size or if changeable length messages have to be handled (Table 1).

A. Organizing the correlation among Sensor agent and monitoring agent

The Sensor Session Point offers three-access points to the sensor agent application (Table 2). The sensor agent up and sensor agent down primitives specify that the sensor agent is began and stopped up, correspondingly. The sensor agent information primitive is exercised to transmit action or status information. The monitor session point requests according to upper layer unite, to report the monitor application about sensor association created, sensor association deleted and to transmit monitoring messages (sensor information received).

The sensor association timeout primitive is exercised to inform the monitor application if a sensor agent unsuccessful to transmit a keep-alive message in the estimated time range. On reception of a sensor agent up primitive, the sensor session point generates an association among the certain sensor agent node identifier and the monitor node identifier (as shown in Table 3), which is recognized beforehand. This association is created by appealing to transmit up information primitive of the sensor transport point with the sensor agent node identifier. If the monitor session point receives up information received primitive, the association is created at the monitor. Analogous method is exercised for the sensor agent down primitive, which erases the association. The sensor agent information primitive is planned to transmit monitoring information primitive. Node registration and verification are out of capacity of this architecture and must be offered by the sensor and monitor application, correspondingly.

If keep-alive messages are exercised, the session layer sustains a timer for each association setting up the next keep-alive message. The timer is begins through the establishment of the association and is set to the keep-alive time (Pa 5.1) minus a pseudorandom offset. If a keep-alive message is due, the transmit monitoring information primitive is raised for the precise association with a possible extra payload offered by the sensor application and the timer is re-initialized as illustrated above. If a monitoring message is transmit for this association, the timer for the next keep-alive message is reorganize to its primary value. Therefore, monitor session point keeps follow of all associations and the most recent legitimate entrance time for a keep-alive message. If this time is surpassed, the sensor association timeout primitive of the monitor application is raised. The newest legitimate entrance time is set on formation of the association and on reception of a received monitoring information primitive from the monitor transport point. It is planned from the existing time, the keep-alive interval (Pa 5.1, as shown in Table 4) and an execution reliant tolerance offset (Pa 5.2).

B. Transport layer

As shown in Table 5, the sensor transport point offers the access points transmit up information; transmit down information and transmit monitoring information to the sensor session point.

Table 1. Presentation layer parameters.

ID	Name	Description
Pa6.1	Fixed message size	Boolean value that determines, if monitoring information is represented in fixed size messages.
Pa6.2	Maximum message size	Unsigned integer value denoting the maximum size of monitoring information to be transmitted. If fixed size messages are used or messages are padded, this is the size of all messages.
Pa6.3	Message padding	Boolean value that is true if a padding is appended to messages smaller than the maximum message size. Is only used if the application does not provide fixed size messages.

Table 2. Session layer interfaces.

ID	Primitive	Parameters
Sensor Session Entity		
Pr5.1	Sensor Agent Up	Identifier of the node that is started and optional information payload.
Pr5.2	Sensor Agent Down	Identifier of the node that is stopped and optional information payload.
Pr5.3	Sensor Agent Information	Identifier of the node sending the information and the information payload to be delivered.
Monitor Session Entity		
Pr5.1	Received Up Information	Node identifier and optional information payload.
Pr5.2	Received Down Information	Node identifier and optional information payload.
Pr5.3	Received Monitoring Information	Node identifier and monitoring information payload.

Table 3. Application layer interfaces.

ID	Primitive	Parameters
Monitor Application Entity		
Pr7.1	Sensor Association Created	*Sensor agent node identifier* for which the association was created.
Pr7.2	Sensor Association Deleted	*Sensor agent node identifier* for which the association was deleted.
Pr7.3	Sensor Information Received	*Sensor agent node identifier* for which information was received and the *information payload*.
Pr7.4	Sensor Association Timeout	*Sensor agent node identifier* for which no keep-alive message was received within the expected time interval.

Table 4. Session layer parameters.

ID	Name	Description
Pa5.1	Keep-alive interval	Unsigned integer value indicating the maximum time between two keep-alive messages (in seconds). If zero, sending entities do not verify the covert channel availability by periodically sending keep-alive messages.
Pa5.2	Keep-alive tolerance	Unsigned integer value giving an implementation dependent tolerance for the keep-alive interval.

Table 5. Transport layer interfaces.

ID	Primitive	Parameters
Sensor Transport Entity		
Pr4.1	Send Up Information	Identifier of the node that is started and data to be sent, which is the data header (including node identifier) and an optional monitoring payload.
Pr4.2	Send Down Information	Identifier of the node that is stopped and data to be sent, which is the data header (including node identifier) and an optional monitoring payload.
Pr4.3	Send Monitoring Information	Identifier of the node that sends the monitoring information and data to be sent, which is the data header (including node identifier) and the monitoring payload.
Monitor Transport Entity		
Pr4.1	Received Segment	Node identifier and the segment, which may be constructed from several frames.

Table 6. Transport layer parameters.

ID	Name	Description
Pa4.1	Segment Type Size	Unsigned integer giving the size of the segment type field in bits.
Pa4.2	Sequence Number Size	Unsigned integer value indicating the size of sequence numbers. If zero, no sequence numbers are sued.
Pa4.3	Message integrity size	Unsigned integer value which is zero if no message integrity check is performed.

Equivalent to the sensor, the monitor transport point releases the primitives received up information, received down information and received monitoring information. The task of the transport layer in this architecture mainly is to carry out Integrity verifications (Pa 4.3).

The channel offered by this architecture is one way (unidirectional) and therefore undependable, which circumvents the complication of a bidirectional protocol and lessens needs that have to be met by an essential communication stage. Though, loss of messages can be identified by the receiver if mutually, dispatcher and recipient, exercise a constant segment (sequence) numbering system (Pa 4.2). The opening sequence number for a fresh association is when the sensor transport point processes transmit up information primitive. The algorithm to establish the initial sequence number from the node identifier and other suitable distinctiveness recognized by the sensor and the monitor is implementation dependent and may be depend on a joint secret, which perform very quickly. A non-trivial task of initial sequence numbers permit the monitor to validate the procedure of generating an association, as the outcome of this test contains in the received up information primitive.

The MIC importance is considered by an implementation dependent function. The input for the MIC computation contains segment header, on the other hand the MIC field is set to all zeros, and segment body.

If a received segment primitive is transmitted by the monitor data link point for a node identifier for which no, the received up information primitive is transmitted former to the received monitoring information primitive. This performance accounts for the one way (unidirectional) channel and will more be submitted to as implicit association creation. The difference among up, down and message segments is initiated for the only reason of organizing the method of allotting sequence numbers and the related resources. The segment of the segment type field (Pa 4.1, Table 6) and the sequence number, if any, and the segment body restraining the monitoring information, because of the deficiency of numerous monitors, no logical addressing of the receiving node is necessary. Additionally, the recognition of multi-hop communication using the covert channel is very implementation dependent as explained below. Therefore, commencing a network layer is considered as a needless overhead and segments are straightforwardly interchanged with the data link layer. If likely at all, multi-hop communication with the monitor using a covert channel can be appreciated with dissimilar method. Flooding may be executed by inserting the covert channel in traffic to all communication associates. Static upstream routes can be characterized as filters, choosing which PDU of the covert channel are exercised for embedding the covert information.

This conclusion may be depend on the destination address of a PDU and allows the mistreatment of further composite routes of the overt channel. Such actions fit in the physical layer of the covert channel, which is implementation dependent.

C. Encoding into Cover traffic

The Data link layer and physical layer are accountable for embedding the covert channel into overt traffic on the other hand characteristics of the physical layer rely on the specific

implementation exercised, the perceptions of the data link layer. These entities executes the assignment of defragmentation, if the greatest size of monitoring information (Pa 6.2) and the size of all headers is bigger than the maximum frame size (Pa 2.2, Table 7).

An implementation establishes the frame size from the maximum number of bits that can be embedded in a cover PDU. If fragmentation is necessary, it can be essential to prefix the frame not only with a node identifier (Pa 2.1) but also with a fragment number (Pa 2.3). The prefix is then exercised to establish the accurate ordering of the frames to get the new segment. It is only necessary if the protocol exercised for traffic encoding do not promise sequential deliverance of data (for example IP) or if the traffic interception is done in such a ways that the arrangement characteristics of a sequential protocol cannot be exercised (for example intercepting TCP traffic in the systems IP stack).

The number of bits presented for representing the fragment number (Pa 2.4) limits the number of likely fragments. Thus, it should be reliable with the highest data size (Pa 6.2), if not, mistakes may be introduced. The number of Cover-PDU necessary to encode a frame to be transmitted (frame queue). The entries of this queue consist of the frame and the newest legitimate encoding time. The most recent suitable encoding time is planned from the time when the first frame of the present segment pushed into the queue a greatest encoding delay (Pa 2.5).

Table 7. Data Link Layer Parameters.

ID	Name	Description
Pa2.1	Node identifier size	Unsigned integer value denoting the size of node identifiers.
Pa2.2	Frame size	Unsigned integer giving the number of bits to be sent in one block. Determines if fragmentation is necessary.
Pa2.3	Fragment numbering required	Boolean value indicating if fragments must be numbered.
Pa 2.4	Fragment number size	Unsigned integer indicating the number of bits available for representing the frame number.
Pa 2.5	Maximum frame delay	Unsigned integer value giving a maximum time for a frame to be sent (in seconds).
Pa 2.6	Frame delay tolerance	Unsigned integer providing an implementation dependent monitor side tolerance offset.

If this time is move beyond, the entire segment is overthrow and the segment encoding timeout primitive is transmitted, which is passed all the way by the layers to the sensor application. The actual encoding of bits is completed by an implementation particular function that recovers a frame from the frame queue and encodes it into the cover traffic.

V. PROTOTYPICAL IMPLEMENTATION FOR WIRELESS SENSOR NETWORKS

In this part of the paper, a very essential implementation of the situations of a wireless sensor networks covert channel is offered. The overt task of the Wireless Sensor Networks installed in this implementation (see Figure 1) is to accumulate temperature information. To guard the network adjacent to theft of sensor nodes, a covert channel is exercised to aware the operator if a node is moved. This prototypical implementation is focused on:

1) Illustrating the effectiveness of a Covert channel for hidden network administration and

2) Representing the practicability of the infrastructural needs of the network covert channel for integrity monitoring. Therefore, these covert channels do not offer strong security adjacent to detection of the covert information.

A. Hardware

The implementation is depending on crossbow MICAz MRP2600 motes, which are a retail edition of the MICAZ MRP2400. The Information is depending on the details of the MRP2400 mote in [9]. These motes exercise an IEEE 802.15.4 CC2420 radio and are working using a Atmega128L microcontroller. For the temperature and acceleration measurements, the crossbow MTS400CA sensor board [10] is added. The specific sensors exercised are the sensirion SHT11 (temperature) and the analog devices ADXL202JE (acceleration). The motes were programmed by means of the crossbow MIB520 USB interface board.

B. Sensor Node Program

The IP Basic Sensor program running successively on the sensor nodes carry out the measurement responsibilities and inform the gateway host using UDP. It is printed in NesC and exercises numerous components offered by TinyOS 2.1. Temperature and acceleration are calculated by the program in intervals of 250-milliseconds. The temperature is accumulated for later on exercise, on the other hand the present acceleration is evaluated. If the dissimilarity among both values is superior to a predefined tolerance, a node progress is identified .because the program is only planned to be a evidence of notion implementation, the forged +ve or -ve resultant from this uncomplicated Algorithm are adequate. Every five seconds, a UDP Datagram contain a measurement statement is transmit to the gateway host. A tailored BLIP stack is exercised to transmit the datagram, which executes the encoding of covert information into the overt measurement reports. Among other, the program exercises the UDP ShellC component, which is also contain d in TinyOS 2.1, to offer a simple CLI that can be accessed from IPV6hosts using UDP .as well to that, the predefined tolerance for the movement detection can be accustomed using the CLI.

C. Gateway serve and Sniffer

In the implementation setup, there are two programs planned to run on the server. Basic_Sensor_server is executes the overt logic job which isthe example of Wireless Sensor Networks. The program produces a socket, which connect to the UDP port specific in the header file, given that it is not episodic by the user, it accepts the measurement reports sent by the Sensor node and produces these reports to the

command line. Basic_Sensor_sniffer can be exercised to decode the Covert Information from the traffic. The sniffer issuing the PCAP library to confine IPV6 traffic on specific interface. It illustrates a text message if the cover traffic restrains the information that a node association was identified by IP Basic Sensor.

VI. COVERT CHANNEL

Here we need a basic covert channel data link layer is enough as the channel is only exercised to transmit out a signal, whether or not the sensor rnode was moved. On the covert channel physical layer, this Information is encoded in the IPV6hoplimit header field. For the purpose of ease, the overt channel in this sensor rnode example engages important overhead concerning the exercise of IPV6and UDP headers evaluated to 32-bit sensor payload. In compare, the covert channel introduces no overhead, as the 8-bit frame is straightforwardly written to the hop limit field, which is of the same size. This is why the covert channel is simple to notice. In addition, it does not offer Integrity proves and it do not facilitate loss detection of associations among Sensor and monitor.

VII. CONCLUSIONS

In the conclusion of this Paper network Covert channels can be exercised to hide the Integrity monitoring for a Wireless Sensor Networks system in distributed system. In this Pa per we also discussed the concrete encoding of secret fragments into Cover traffic is a very important and vast field for wide research that is at the best of my knowledge presented in section 3. Nevertheless, a employment of a Covert channel in the situations of Integrity monitoring needs a definite amount of robustness, which is extremely dependent on the employment platform and the specific type of Cover traffic. This feature is not offered by the greater Part of the proof of concept implementations.

The model of a network Covert channel shows in section 4offers a modular explanation of the essential responsibilities to make certain robust Covert Communications between Sensor Nodes and a monitor. The layer architecture of the model offers elasticity for specific needs of diverse operation platforms or diverse types of Cover traffic. From the explanation of numerous channel features it can be seen that there is a trade-off among robustness and capacity of a Covert channel.

REFERENCES

[1] Clare, Loren P., Gregory J. Pottie, and JonathanAgre (1999), "Self-Organizing Distributed Sensor Networks", Proc. SPIE Aerosense 99.

[2] Dargie, W. and Poellabauer, C., "Fundamentals of wireless Sensor networks: theory and practice", John Wiley and Sons, 2010 ISBN 978-0-470-99765-9, pp. 168–183, 91–192.

[3] Sohraby, K., Minoli, D., Znati, T., "Wireless Sensor networks: technology, protocols, and applications, John Wiley and Sons", 2007 ISBN 978-0-471-74300-2, pp. 203–209

[4] C. Shen, C. Srisathapornphat, and C. Jaikaeo, "Sensor Information Networking architecture and Applications," *IEEE Pers. Commun.*, Aug. 2001, pp. 52–59.

[5] S. Tilak, N. Abhu-Gazhaleh, and W. R. Heinzelman, "A Tax Anomy of Wireless MICroSensor Network Models," *ACM SIG MOBILE Mobile Comp. Commun. Rev.*, vol. 6, no. 2, Apr. 2002, pp. 28–36.

[6] I. Akyldiz *et al.*, "A Survey on Sensor Networks," *IEEE Commun Mag.*, vol. 40, no. 8, Aug. 2002, pp. 102–14.

[7] C. Krauß, F. Stumpf and C. Eckert, "Detecting Node Compromise in Hybrid Wireless Sensor NetworksUsing Attestation techniques," Proceedings of the 4th European conference on Security and Privacy in Ad-Hoc and Sensor Networks, 2007.

[8] T. G. Handel and M. T. Sandford, "Hiding Data in the OSI Network Model," Proceedings of the First International Workshop on Information Hiding, Vol. 1174, 1996, pp. 23-38. doi: 10.1007/3-540-61996- 8_29

[9] Crossbow Technology Inc., "MPR-MIB Users Manual", June 2006.

[10] Crossbow Technology Inc., "MTS/MDA Sensor Board Users Manual," June 2006.