Volume 2, No. 8, August 2011
Journal of Global Research in Computer Science
ISSN-2229-371X
RESEARCH PAPER
Available Online at www.jgrcs.info

WIRELESS SENSOR NETWORK BASED TRAFFIC MONITORING; OVERVIEW AND THREATS TO ITS SECURITY

Sareh Nasaghchi Kheirabadi [*1], Dr Nitin. M. Kulkarni [2], Dr Arvind. D. Shaligram [1]
[1]Department of Electronic Science, University of Pune, Pune, India
snasaghchi@yahoo.com [*1]
[2]Department of Electronic Science, Fergusson College, Pune, India

Abstract: The increased number of vehicles has caused a series of economic and social problems across the world. The economic viability of using wireless sensor networks to gather roads traffic monitoring data for intelligent transportation systems (ITS) becomes increasingly attractive. ITS systems are subject to security threats like any other information technology systems. Security should be considered as an integral part of ITS planning and deployment. There is a compelling need to identify and address the most severe security threats specific to the traffic monitoring sensor network. Here an analysis of possible threats to traffic monitoring system is presented using the European Telecommunications Standards Institute's (ETSI's) methodology and threats that pose the most significant risk to the system are identified. Necessary security services that satisfy the system's security objectives are listed.

Keywords: Wireless sensor network, Traffic monitoring, Security attacks, Threat analysis.

INTRODUCTION

As the cost of embedded devices, sensors, and wireless networking decreases, the economic viability of intelligent services that sense conditions in the physical world and trigger responses to them becomes increasingly attractive. Examples of such systems include telematics systems deployed in fleets to improve safety and fuel efficiency, environmental sensor networks deployed for security or community health protection and highway-based sensor networks for intelligent transportation systems [1]. At present, there is a dearth of discussion on security issues pertaining to sensor communications, although some issues have been addressed. ITS systems are subject to security threats like any other information technology systems.

Experience has shown that it is very difficult to implement security measures properly and successfully after a system has been developed, so security should be integrated early in the system lifecycle.

Given different security requirements in different applications, there is a compelling need to identify and address the most severe security threats specific to the traffic monitoring sensor network which is done in this work. To do so, the European Telecommunications Standards Institute's (ETSI's) methodology is used, where identified threats can be ranked as critical, major or minor depending on their likelihood of occurrence and impact on the user or the network and the threats that pose the most significant risk to the system are identified. Also necessary Security services that can blunt or remove the threats and satisfy the system's security objectives are listed.

Section 2 presents an overview of traffic monitoring. Section 3 describes various available monitoring devices. In section 4 we describe the security requirements in the network. Section 5 outlines the methodology used to rank the threats. Section 6 provides an analysis of the identified threats along with their risk assessments and at the end concludes the paper.

NEED FOR TRAFFIC MONITORING

Rising traffic levels and increasingly busier roads are a Common feature across the globe. Consequently, there is an increasing requirement to develop intelligent traffic surveillance systems that can play an important role in highway monitoring and road management systems. Improving the efficiency of transportation systems has tremendously economical and environmental impacts. In May 2006, the U.S. Department of Transportation announced that 'congestion is one of the single largest threats to our economic prosperity and way of life' and it costs America an estimated $200 billion a year. The congestion problem is getting worse each year. In 2007, urban Americans travel an extra 4.2 billion hours due to congestion, which is a 20 times increase of 220 million extra hours from 2004. The situation is even worse in populous developing countries such as China and India as they are experiencing fast economic growth. Intelligent traffic control is very important in addressing traffic congestion [2].

ITS tries to provide immediate services to all users, regardless of the degree of special instrumentation available to them. Basic service will be provided to the users through publicly available channels such as Dynamic Message Signs (DMS) and Highway Advisory Radio (HAR). Also the ITS benefits can be available to large numbers of commercial and private travelers at no cost or a small cost from better regional travel information broadcast by commercial AM/FM/Cable operators. In-vehicle route guidance is another benefit of ITS. The infrastructure (the ISP) selects the best route based upon the traveler route request to minimize the travel time. Any reduction in time between the occurrence of an injury accident and the arrival of medical help has a substantial impact on survivability. In the high-end state architecture, emergency vehicles will have their routes selected by the infrastructure, and those routes will be communicated to the Traffic Management service package

for priority signal service for the emergency vehicles (with minimal disruption to the rest of the transportation network).

Also intersection collision avoidance can be provided by determining the probability of a collision in the intersection and sending appropriate warnings and/or control actions to the approaching. Information related to surface weather can provide automated systems to apply anti-icing materials, disperse fog, etc. in adverse conditions.

One user group of the Traffic Information System can be traffic system planners, to effective management of road traffic, where information regarding the speed and volume of traffic is useful. This enables alternative routes to be planned in response to accidents or road closures and to attempt to relieve congestion, perhaps by altering speed limits [3]. Another user group can be researchers who develop traffic information systems. Also drivers keen to know about traffic in general and traffic jams in particular need the real time traffic information. Radio stations can use this information to broadcast alerts about traffic jams.

Almost all of these systems are myopic, focusing strictly on current conditions**.** Yet the data collected by the sensors can provide considerable information when viewed over time. In [4] the writers investigate and demonstrate several applications that employ traffic monitoring system data over time to show the added benefit of the given system.

Not only new intelligent transportation systems (ITS) require real-time knowledge of traffic movement to be effective, but also this information is required for proper design of roadways. Protection of aging infrastructure requires detailed understanding of the number, type, and weight of the vehicles using roads and bridges. The sacrificial layer should neither be replaced too soon, leading to unnecessary costs, nor too late, risking more serious damage to the underlying structure of the road. An accurate determination of the volume of traffic on a particular road section is therefore essential [3]. These needs and others strain available resources within the industry, pushing technology to develop better, faster ways to accurately measure and record vehicular data and transmit this information reliably to where it can be safely analyzed [5].

NEED FOR SENSOR NETWORK

It is clear that information regarding the speed, weight, volume and type of traffic can all be used to help with an effective road traffic management program. One of the most important part of ITS is the equipment distributed on and along the roadway that monitors and controls traffic and manages the roadway. Currently, collecting traffic data for traffic planning and management is achieved mostly through wired sensors. One of the most conventional (and popular) consists of inductive loop detectors buried in asphalt. Less "intrusive" techniques include video image processors, microwave radar, infrared laser radar, and acoustic/ultrasonic devices [6]. But this method has its own problems. The ultrasonic sensor is very sensitive to the weather. Inductive loop typically affects the traffic during installation and are prone to breakage as a result of other construction. Many sections of road are overseen by video cameras. The images from these cameras are fed to central points to be analyses to provide information regarding vehicle speed and type and traffic volume. However, due to the complexity of the images, it is not always possible to reliably automate the analysis of the data received, meaning that they must be studied visually. There is a limit to how many images can be analyzed in this way. Furthermore, the quality of the images collected may be influenced by weather conditions. Fog or rain can obscure the field of view of the cameras, as can high vehicles, and high winds can cause the cameras to vibrate. The commissioning costs of video camera systems for traffic monitoring can also be high [7]. The equipment and maintenance cost and time-consuming installations of existing sensing systems prevent large-scale deployment of real-time traffic monitoring and control.

Another way of monitoring traffic that these days increasingly makes research topic is to use probe vehicles to monitor traffic: they can automatically report position, travel time, traffic incidents, and road surface problems to a telematics service provider. This kind of traffic-monitoring system could provide good coverage and timely information on many more roadways than is possible with a fixed infrastructure such as cameras and loop detectors [7]. However, this approach's drawback is that for a lengthy time period, only a small subset of vehicles will be equipped, which is not sufficient for the real time traffic monitoring. An additional obstacle is the negative perception that the population might have about such mechanisms, especially the feeling of being permanently monitored by some arbitrary authority [6]. This may cause drivers or third parties to modify the hardware or software to report incorrect vehicle positions or speed readings, which leads to incorrect data collection about traffic.

Small wireless sensors with integrated sensing, computing, and wireless communication capabilities offer tremendous advantages in low cost and easy installation and offer the potential to significantly improve the efficiency of existing transportation systems. A networked wireless sensor system can be used to collect and process real-time information on many characters of roadway including vehicle detection, tracking, speed, length and weight in motion where these information can be used in cases where there are regulations relating to maximum allowable weights for heavy goods vehicles which are borne out of concerns for. They also can be used to collect information regarding type of vehicles using a particular section of road. This may be to prevent unsuitable vehicles such as heavy goods vehicles from using rural roads or to plan future road building schemes. Also they can collect information on vehicle emission, road surface weather and detecting hazardous materials. There are researches which tried to use WSN for these purposes [8 - 10]. Successful development of these systems will significantly reduce traffic congestion, travel time, fuel consumption, and air pollution.

In [11], the authors examined the detection capability of sensor motes using magnetic sensors. Their network could provide a detection rate of 99 percent; and achieve 90 percent accuracy in average vehicle length and speed estimates with a single sensor. They used the localized

change associated with the magnetic sensor to classify the vehicles based on the magnetic signature without incorporating the length with 60 percent accuracy. Their experiments with two nodes six feet apart indicate speed estimates with an accuracy exceeding that obtained by a video camera (because the nodes provide a resolution of 128Hz vs. the 30Hz video frame rate)**.** The (correct) detection rate of the sensor network was 98% compared with 86% by the inductive loop. Also they achieved 80 percent correct classification of trucks by measuring their weigh-in-motion (WIM), without using vehicle length.

NEED FOR SECURITY PROTECTION

Wireless provides an excellent communication medium but it also has risks. Wireless communications are easier to intercept than wire-based. Rather than digging up cable or gaining physical access to a router, a malicious user can sit in a parking lot and pick up communications from several miles away. A malicious user can also create and interject his own signals wirelessly. Therefore it is important that the communications for traffic monitoring be safe and secure. This will help prevent the accidental or malicious actions that can cause disruption.

Although malicious attacks on traffic monitoring might sound far-fetched, they appear quite plausible if you consider the gray market devices people now buy to reduce travel time (such as infrared transmitters to change traffic lights). These new devices might manipulate the congestion index to divert traffic away from a road to reduce a particular driver's travel time or toward a particular roadway to increase revenue at a particular store. Other service providers might also try to dilute the information quality of a competing traffic-monitoring service [7].

For four reasons, securing the ITS communications network during the system design phase is crucial: First, system design presents the most effective phase at which to limit exposures. Second, considering security early can limit research expenditures on proposals that are unlikely to be securable. Third, ignoring the possibility of attacks can lead to incorrect conclusions about system robustness. Finally, security is crucial to garnering governmental approval and consumer acceptance [12].

Security Objectives in Traffic Monitoring:

The main security principles or objectives apply to any security program - including ITS security – are Confidentiality, Integrity and Availability. All security services are implemented to support one or more of these objectives. Similarly, all threats undermine one or more of these objectives. How well a security system performs, can be measured by the extent to which it meets the desired objectives.

The *Confidentiality* objective ensures that information is not disclosed to unauthorized individuals, processes, or systems (e.g., protecting trucking company records). The monitoring data are usually not security sensitive data to be kept confidential so in traffic monitoring end to end confidentiality is not a big concern.

The *Integrity* objective ensures the accuracy and reliability of information and systems, and defines the level of protection from unauthorized intentional or unintentional modifications. This objective is related to auditing accountability, authentication, and access control services for sensitive information.

The *Availability* objective ensures that systems and information are accessible and usable to authorized individuals and/or processes.
Table 1 summarizes these security objectives and their importance in ITS [13].

Table 1. The security objectives and their classifications for the wireless sensor network based traffic monitoring

Objective	*Classification*	*Description*
Confidentiality	Low	Information is generally available to people.
Integrity	High	Unauthorized or unintended modification of the information could result in degradation of traffic control.
Availability	High	Loss of the information could make ITS services unavailable to the users.

Potential Security Considerations in Wireless Sensor Network Based Traffic Monitoring:

Roadway Monitoring Data Security: Most traffic monitoring data are less sensitive, containing road way condition information that is not confidential and does not require special security measures. The required availability of traffic monitoring data must be considered based on its application. In some cases, these data are used for off-line applications where short-term loss of availability will not cause serious impact to the transportation system. The most critical objective for traffic monitoring is data integrity. Since the archived data of traffic monitoring are frequently used to measure performance of the transportation system and provide data that supports operations and planning, the accuracy and reliability of the data contained in the archive is paramount. Also the online traffic monitoring data is used for traffic reports, Information Service Providers and drivers rout selection which requires integrity of data.

An intersection is a basic node of the urban traffic network. Due to the randomness of the traffic flow, the periodical signal control method is unable to adapt the signal control to the dynamic traffic flow, and it only works for the less busy intersections [14]. In real-time adaptive traffic light control, traffic light controllers use sensor's real-time road traffic data and make real-time decisions on traffic light duration and sequences. A commonly used performance metric is the average trip waiting time (ATWT). The trip waiting time of a vehicle is the time it spends waiting at intersections. So the integrity and availability of the traffic sensor data has important effect on the accurate traffic signaling in these systems.

Traffic monitoring data may be safety critical if this information is used to monitor for incidents or dangerous road conditions. Although the more likely threats to sensor and surveillance information involve inadvertent loss or corruption of the provided information, malicious tampering is also possible. Also dependences with traffic signal systems and future systems that may support automated

vehicle control systems, these data becomes safety critical, since improper operation of these systems can directly endanger motorists. The security services should be established so that these systems operate with very high levels of integrity and availability.

Hazardous Materials Detection Data: Vapor and trace detection systems are two types of chemical sensor systems in use. Vapor detection systems essentially sniff the air e.g. inside cargo shipping centers, and analyze the chemical makeup of the trace elements. These devices are valuable because of their ability to detect explosives from a distance. Because explosive materials are often volatile, their elements easily evaporate into the air. Some perpetrators may attempt to wrap explosives well to avoid detection, but the trace amounts on their fingers or gloves while wrapping can still be detected.

Trace detection systems require operators to wipe the cargo with a collection strip, which is then inserted into a detection machine. The particulate matter from the collection strip is then analyzed for traces of explosives [15].

security sensitive hazardous materials Cargo content information should be protected from unauthorized access for knowledge of this information, as they could target the vehicle for hijacking or terrorist attack and so needs to have a relatively high degree of confidentiality in order to safeguard the information. In addition, it is important that the information about the commercial vehicle and its cargo is available to the Commercial Vehicle Administration subsystem. The integrity of the information from the commercial vehicle is also important to prevent deceptive practices.

Emergency Vehicles: The functions of Emergency vehicles are frequently safety critical since they directly impact the ability to provide an effective response to emergencies, which in turn impacts public safety.

Emergency vehicles including police cruisers, command vehicles, various types of fire apparatus, service patrol vehicles, ambulances, towing and recovery vehicles, and many different specialized response vehicles, may have very different security requirements, depending on the functions supported, the data that is stored, and the mission criticality of the services provided. For example, maintaining confidentiality of police vehicle locations is a public safety concern and frequently a key security objective. Tow vehicle locations are generally not a public safety concern, but tow truck operators may still want to prevent unauthorized vehicle location disclosure for business reasons. Finally, the current location of a service patrol vehicle may not be considered to be particularly sensitive.

Also some emergency vehicles such as the police car, the fire engine, the ambulance that have the privilege of passing the intersection need the special treatment.

Vehicle Emissions: The sensors can collect vehicle emissions data and regional air quality data that are generally not sensitive to public disclosure. Also, while air quality is extremely important to everyone, the emission are generally not mission critical and could be lost or delayed for short periods of time without serious implications for public safety or operational efficiency of the transportation system. In most cases, normal precautions that are taken to protect data integrity will also suffice here since the threat of inadvertent or malicious tampering with data is not particularly high.

There are scenarios where the security associated with Emissions Management will be more significant. For example, data integrity and confidentiality are more significant if the specific emissions sensing system is identifying emissions/pollution violators. This information is both sensitive and subject to tampering. In most cases, data availability will not be critical, but specific data may require higher availability if the network of sensors and data collected are relied upon to detect and report dangerous levels of pollutants or other airborne materials in emergency situations. Table 2 summarizes the security threats and their importance to the system [13].

Table 2. The security threats and their importance in the wireless sensor network based traffic monitoring

Threat	*Importance*	*Threat Description*
Deception	High	A circumstance or event that may result in an authorized entity receiving false data and believing it to be true.
Disclosure	Low	A circumstance or event whereby an entity gains access to data for which the entity is not authorized.
Disruption	High	A circumstance or event that interrupts or prevents the correct operation of system services and functions.

Security Threats:

Among different communication layers, mainly network layer protocol (i.e. routing protocol) suffers from many attacks like; spoofing or altering the route information, selective forwarding, sinkhole attack, Sybil attack, wormhole attack, HELLO flood attack, etc. These attacks cannot be prevented by using a simple link layer security (using a global shared key), since the sensor nodes are very susceptible for node capture and in presence of the insider attacker or compromised nodes more secured techniques are required [14]. Karlof and Wagner [16] analyzed many routing protocols, and showed that all of them are vulnerable to different kind of attacks. After that many tried utilize security solution in routing protocols [17 - 22], but none of them are application specific. To achieve an efficient security mechanism for resource constrained sensor network it is important to have an application specific view to the problem. What we want to protect is sometimes very different from one application to another application. Noting to the specification of the application and the actual requirement of it, leads to a much more accurate and efficient system. Here we focus on threat analysis to the traffic monitoring application by considering the potential threats, the likelihood of occurrence, the system's vulnerability to those threats, and the damage that may occur if the threat is realized. The threat analysis ultimately identifies the threats that pose the most significant risk to the system. Security services can then be identified that are necessary to blunt or remove the most significant threats and satisfy the system's security objectives.

ANALYSIS METHODOLOGY

In 2003, the European Telecommunications Standards Institute (ETSI) developed a methodology for analyzing security threats to its meta-protocol, Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) [23]. This methodology allows for identified threats to be ranked in terms of risk, using estimated values for the likelihood of occurrence and impact upon the user or system.

The *likelihood* of occurrence of the threat indicates whether theoretical and practical knowledge is available for attackers to carry out an attack. Three levels of likelihood are defined with an associated numerical value: *Likely* (3) – all elements in place; *Possible* (2) – some elements in place; *Unlikely* (1) – important elements missing.

Although the *impact* of a threat has no bearing on whether an attack occurs, it can indicate if the threat is serious enough to warrant further research into possible countermeasures. The values associated with the impact are the following: *High* (3) – serious consequences for the user or network; *Medium* (2) – short-term outages; *Low* (1) – minor consequences for the user or network.

The *risk* is calculated as the product of the numerical values of the likelihood and impact. The categories in which the risk is deemed to fall are defined as: *Critical* (9, 6) – countermeasures must be devised without delay; *Major* (4) – the threat will eventually require attention; *Minor* (3, 2, 1) – the threat can be ignored in the short term.

In [24], Barbeau has used the definitions provided in [23] to further break down the likelihood component into its two natural components: the technical difficulty in carrying out the threat and the motivation or potential gain for the attacker. The values for technical *difficulty* are defined in terms of whether or not the threat has previously been considered in theory or in practice: *None* – a precedent for the attack exists; *Solvable* – the attack is theoretically possible; *Strong* – theoretical elements missing. The levels for *motivation* include: *High* – significant gains for attacker; *Moderate* – service disruption only; *Low* – no significant gains. The technical difficulty and motivation associated with a given threat can be used with its impact to determine the risk assessment, as depicted in **Table 3** [25].

Table 3. Risk Assessment

<table>
<tr><th rowspan="2">Motivation</th><th rowspan="2">Difficulty</th><th rowspan="2">Likelihood</th><th colspan="3">IMPACT</th></tr>
<tr><th>High</th><th>Medium</th><th>Low</th></tr>
<tr><td rowspan="2">High</td><td>None</td><td rowspan="2">Likely</td><td colspan="2" rowspan="3">Critical</td><td rowspan="4">Minor</td></tr>
<tr><td>Solvable</td></tr>
<tr><td rowspan="2">Moderate</td><td>None</td></tr>
<tr><td>Solvable</td><td>Possible</td><td>Major</td></tr>
<tr><td>Low</td><td>Any</td><td rowspan="2">Unlikely</td><td colspan="3" rowspan="2">Minor</td></tr>
<tr><td>Any</td><td>Strong</td></tr>
</table>

THREAT ANALYSIS

In this analysis, the focus is on the most basic security attributes to be preserved in ITS: integrity and availability. A network of wireless sensors without security protection is considered (or with simple link layer protection, as there is not much difference between them. Once the keying material of a sensor gets compromised due to tampering, the whole network is compromised.). The collated list of threats, organized by risk category, can be found in **Table 4.** The defense technique of the threats is listed in **Table 5.**

Table 4. Threat Analysis

Threat	*Motivation*	*Difficulty*	*Likelihood*	*Impact*	*Risk*
Incorrect Data Injection (replay attack or altering data)	High	Solvable	Likely	High	Critical
DOS	Moderate	Solvable	Possible	Medium	Major
Denial of sleep	Moderate	Solvable	Possible	High	Critical
Selective forwarding (blackhole, sinkhole, wormhole or sybil attack)	High	Solvable	Likely	High	Critical
Malwares	Moderate	Solvable	Possible	High	Critical

Table 5. Required security solution for a secure traffic monitoring application

Threat	*Countermeasure*
Incorrect data injection	Message authentication code and antireplay techniques
DoS	authentication and antireplay protection
Denial of sleep	authentication and antireplay protection
Selective forwarding	authentication techniques and secure routing protocols, authentication techniques and Geographic routing protocols
Malwares	authentication techniques

Threats to Integrity:

Incorrect Data Injection: It is possible that a rogue insider may attempt to inject false traffic information or traffic urgent messages into the network for the purpose of suppressing traffic lights to shorten his travel time, manipulating the flow of traffic to clear a chosen route or even for the purpose of disruption in the network. This may happen by injecting false data, replaying the previously transmitted data or altering the message while passing through routing path. The solvable technical difficulty involved in carrying out this threat, potential gains for an attacker and the high level integrity requirement to traffic monitoring application, the impact of the threat on system indicated a critical one. Message authentication code and antireplay techniques have to be used to prevent this threat.

Threats to Availability:

Threats to the availability and consistent behavior of the sensor network include denial of service (DoS) attacks, Denial of sleep attacks, selective forwarding and Malwares. Since ITS relays on the real time properties of traffic monitoring, absence of availability may results in improper signal functioning and increasing traffic jams. Also lose of availability is more sever, when the routed message is an emergency message to report about some urgent situation, for example detection of presence of hazardous materials in a passing vehicle or presence of an ambulance waiting for a traffic light to become green.

DoS: DoS attacks render the network unavailable to its users. It is an attack that can happen in any layer of communication protocols, for example by flooding the nodes with messages or by jamming signals at the physical layer. These attacks can be carried out either by network insiders turned rogue or by outsiders to the network.

By jamming the physical layer of the network, an attacker can hamper message delivery, thereby compromising the applications which depend upon it. Techniques for identifying jamming attacks include statistically analyzing the received signal strength indicator (RSSI) values, the average time required to sense an idle channel (carrier sense time), and the packet delivery ratio (PDR) [26]. We do not consider attacks to physical layer in this work.

One way to incapacitate the sensor network is to artificially generate a high volume of false messages that the network's nodes, cannot sufficiently process the superfluous data resulting in loosing data. Given that DoS represents a disruption rather than an opportunity for gain, the motivation required on the part of an attacker is rated as moderate according to the criteria provided in Section 5.The technical difficulty involved is solvable, given that it is theoretically possible. Since DoS would result in temporary outages, the impact on the network is ranked as medium, and according to Table 3, the threat is assessed as major. Defense techniques include authentication and antireplay protection [27].

Denial of Sleep: A clever denial-of-sleep attack that keeps the sensor nodes' radios on would drain the batteries in only a few days. As Energy is the most precious resource in sensor network the impact of this threat to the network is ranked as high. The solvable technical difficulty leads to assess this treat as critical. Defense techniques include authentication and antireplay protection [27].

Selective Forwarding: This action may be created by insider of the network which is a part of the routing path. Almost all threats to the routing protocol (Spoofing, altering, or replaying routing information, sinkhole, wormhole or sybil attack) may result to a malicious node to make itself part of many routes. A simple form of this attack is when a malicious node behaves like a black hole and refuses to forward every packet he sees. However, such an attacker runs the risk that neighboring nodes will conclude that she has failed and decides to seek another route. A more subtle form of this attack is when an adversary selectively forwards packets. Considering this kind of attack may be mostly used to drop urgent packets, rather than usual traffic data packets, the motivation of this attack is ranked as high. The technical difficulty is solvable since it is theatrically possible. The impact on the system is critical. Implicit acknowledgement and multi path routing are techniques to defense this attack. More efficient technique is to prevent a malicious node to become a part of routing path by use of authentication techniques and secure routing protocols. Geographic routing protocols alone cannot defense this threat since the location information of node is subject to attack and change and cannot be trusted.

Malwares: The introduction of malware, such as viruses or worms, into the sensor network has the potential to cause serious disruptions to its operation, since the sensor nodes are expected to receive periodic software and firmware updates. The associated motivation is ranked as moderate because it consists of a disruption in service. Since the threat is theoretically possible, the technical difficulty is a solvable one if countermeasures are not in place. The impact on the user is considered high due to the resulting long-lasting outages. As a result, the malware threat is ranked as critical. Defense to these attack are highly secure authentication techniques.

CONCLUSION AND FURTHER WORK

In this work, the inherent security in sensor network for traffic monitoring application are identified and the identified threats are ranked according to the European Telecommunications Standards Institute's (ETSI) threat analysis methodology. Possible countermeasures to the most critical threats are also discussed. According to Table 5 the most sever security requirements in this application are: authentication, antireply and message authentication code
As further work, a secure data communication protocol and algorithm for Wireless Sensor Networks (WSNs) that can operate correctly in traffic monitoring application will be proposed. Considering the energy and hardware constraints of the sensor nodes, an efficient protocol is required.

REFERENCES

[1]. JuHee Bae, Christopher Howson, WonIl Lee, Jonathan Munson, Young Ju Tak, "Architecture and Performance of a Scalable Telemetry Acquisition and Distribution Infrastructure", 2007 International Conference on Intelligent Pervasive Computing .

[2]. Malik Tubaishat, Peng Zhuang, Qi Qi and Yi Shang, "Wireless sensor networks in intelligent transportation systems", Wireless Communications and Mobile Computing, 9:287–302, 2009.

[3]. "Road traffic monitoring system", United States Patent 7024064.

[4]. Keith A. Redmill and Benjamin A. Coifman, "System Management and Monitoring - Temporal Evaluation of Freeway Management Systems", Proceedings of the IEEE ITSC. 2006 IEEE Intelligent Transportation Systems Conference

[5]. Mark P. Gardner, Fugro-Bre, "Highway Traffic Monitoring", Committee on Highway Traffic Monitoring, Chairman: David L. Huft, South Dakota Department of Transportation.

[6]. Jean-Pierre Hubaux, Srdjan Capkun, Jun Luo, "The Security and Privacy of Smart Vehicles", IEEE Security & Privacy, 2004, IEEE.

[7]. Baik Hoh, Marco Gruteser, Hui Xiong, Ansaf Alrabady, "Enhancing Security and Privacy in Traffic-Monitoring Systems", PERVASIVE computing, October–December 2006, IEEE.

[8]. Yuhe Zhang, Xi Huang, Li Cui1, Ze Zhao, "Design and Evaluation of a Wireless Sensor Network for Monitoring Traffic". The 14th World Congress on Intelligent Transportation Systems (WCITS'07), 2007.

[9]. Cory Sharp, Shawn Schaffert, Alec Woo, Naveen Sastry, Chris Karlof, Shankar Sastry. David Culler, "Design and Implementation of a Sensor Network System for Vehicle Tracking and Autonomous Interception", Proceedings of the Second European Workshop on Wireless Sensor Networks, 2005, IEEE

[10]. Zhijun Shang, Haibin Yu, Jun Wang, "Design and implementation of a vehicle detection testbed using wireless sensor networks", Proceedings of International Conference on Communications, Circuits and Systems, 2005, IEEE.

[11]. Sing Yiu Cheung, Sinem Coleri Ergen and Pravin Varaiya, "Traffic Surveillance with Wireless Magnetic Sensors", Proceedings of the 12th ITS World Congress (2005).

[12]. Jeremy Blum and Azim Eskandarian, "The Threat of Intelligent Collisions", Published by the IEEE Computer Society, January / February 2004

[13]. National ITS Architecture Security, Prepared by the Architecture Development Team, US Department of Transportation, May 2007.

[14]. Chen Wenjie, Chen Lifeng, Chen Zhanglong, Tu Shiliang, "A Real-time Dynamic Traffic Control System Based on Wireless Sensor Network", Proceedings of the 2005 International Conference on Parallel Processing Workshops (ICPPW'05), 2005, IEEE.

[15]. Ryan Fries, Mashrur Chowdhury, Jeffrey Brummond, "Transportation Infrastructure Security utilizing Intelligent Transportation Systems", John Wiley & Sons, Inc publication, 2009.\

[16]. Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", Ad Hoc Networks, vol 1, issues 2-3, September 2003.

[17]. Leonardo B. Oliveira, Adrian Ferreira, Marco A. Vilaca, Hao Chi Wong, Marshall Bern, Ricardo Dahab, Antonio A.F. Loureiro, "SecLEACH—On the security of clustered sensor networks", Signal Processing 87 (2007) 2882–2895, Elsevier.

[18]. Nidal Nasser, Yunfeng Chen, "SEEM: Secure and energy-efficient multipath routing protocol for wireless sensor networks", Computer Communications 30 (2007) 2401–2412, Elsevier.

[19]. Yunfeng Chen and Nidal Nasser, "Enabling QoS Multipath Routing Protocol for Wireless Sensor Networks", IEEE International Conference on Communications, 2008. ICC '08, IEEE.

[20]. Kun Zhang, Cong Wang, Cuirong Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management", 4th International Conference on Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08, IEEE.

[21]. Suraj Kumar Sharma, Sanjay Kumar Jena, "SCMRP: Secure Cluster Based Multipath Routing Protocol for Wireless Sensor Networks", Sixth International Conference on Wireless Communication and Sensor Networks (WCSN), 2010, IEEE.

[22]. Yang Yang, Enjian Bai, Jia Hu, Wenqiang Wu, "MRBCH: AMulti-Path Routing Protocol Based on Credible Cluster Heads for Wireless Sensor Networks", Int. J. Communications, Network and System Sciences, vol 3, pages 689-696, 2010.

[23]. ETSI. Telecommunications and internet protocol harmonization over networks (TIPHON) release 4; protocol framework definition; methods and protocols for security; part 1: Threat analysis. Technical Specification ETSI, 2003.

[24]. M. Barbeau: WiMax/802.16 Threat Analysis. Proceedings of the 1st ACM International Workshop on QoS and Security for Wireless and Mobile Networks (Q2SWinet), 2005.

[25]. Christine Laurendeau and Michel Barbeau, "Threats to Security in DSRC/WAVE", T. Kunz and S.S. Ravi (Eds.): ADHOC-NOW 2006, LNCS 4104, pp. 266–279, Springer, 2006

[26]. W. Xu, W Trappe, Y Zhang, T Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, ACM Press, 2005.

[27]. David R. Raymond and Scott F. Midkiff, "Denial-of-service in Wireless Sensor Networks: Attacks and Defenses", Pervasive Computing, IEEE, 2008.

