International Journal of Advanced Smart Convergence Vol.7 No.4 174-184 (2018)
http://dx.doi.org/10.7236/IJASC.2018.7.4.174

IJASC 18-4-22

A Study of a Seamless Handover Support for WSN based Information Transmission in Structural Health Monitoring Systems

Byungjoo Park

Department of Multimedia Engineering, Hannam University, Daedeok-gu, Daejeon, Korea
bjpark@hnu.kr

Abstract

The efficiency and safety of social-overhead capital (SOC) public infrastructures have become an eminent social concern. In this regard, a continuous structural health monitoring has been widely implemented to oversee the robustness of such public infrastructures for the safety of the public. This paper deals with the analysis of a distributed mobility management (DMM) support for wireless sensor network (WSN) based information transmission system. The partial DMM support separates the data and control plane infrastructures, wherein, the control plane is managed by a particular mobility management network entity, while the data plane is distributed by the mobility anchors. The system will be able to optimize the information transmission for a wireless structural health monitoring of SOC public infrastructures specifically designed for bridges, and thus, guarantees the safety of public commuters.

Keywords: *distributed mobility support, WSN, information transmission system, social overhead capital (SOC)*

1. Introduction

Nowadays, the SOC public infrastructures must be safeguarded with a real-time and continuous structural health monitoring (SHM) to provide safety for the public. It becomes almost a necessity for every SOC public infrastructure and most recently being widely applied to bridges. Management of bridges greatly benefit from SHM through a continuous evaluation, assessment, and real-time monitoring. In this regard, the utilization of WSNs has been widely adopted as a major SHM solution to address and manage such SOC public infrastructures. The installed sensors are capable of monitoring both the environmental conditions as well as calculating the bridge's external loads. The sensors may include wind pressure sensors; anemometers to measure wind speed and direction; seismograph for measuring ground motions; weather station to measure air temperature, barometric pressure, air temperature, and rainfall; accelerometers, tilt meters, GPS, video cameras, motion sensors, vibration sensors, and other environmental condition measuring devices. The signals generated by these sensors are relayed into gateways to be transmitted to the central monitoring station for analysis.

Since moving vehicles tend to regularly change its point of attachment as it passes through bridges,

Manuscript Received: Oct. 28, 2018 / Revised: Nov. 9, 2018 / Accepted: Nov. 15, 2018
Corresponding Author: bjpark@hnu.kr
Tel: +82-42-629-8489, Fax: +82-42-629-8489
Department of Multimedia Engineering, Hannam University, Daedeok-gu, Daejeon, Korea

mobility management becomes one of the most essential concern in the success of wireless structural health monitoring systems designed to safeguard bridge infrastructures. Various optimizations for handover mobility management were standardized in order to provide a robust mobility support for different wireless systems across a heterogeneous network environment. The use of the standard mobile internet protocol version 6 (MIPv6) to provide mobility management support is not recommended for the implementation of any wireless systems anymore, specifically if human lives are at stake. Information transmission in such systems is very critical that must be conveyed in real-time and continuously.

The centralized systems of mobility management may offer an organized control and handover management for wireless network systems, however, the use of a single centralized network entity poses a number of issues in terms of data traffic distribution. This entity can become a bottleneck in such a way that it can become a center of congestion for data traffic. Moreover, a single point of failure is a major concern as well as for security issues. This paper deals with the implementation of distributed mobility management based mobility support in handling the handovers of moving vehicles passing through bridges. The advantages of DMM to support the mobility handovers for information transmission in structural health monitoring systems were utilized in order to optimize the transmission of measured structural health information.

The rest of this paper is organized as follows: Section 2 provides an overview of the structural health monitoring for SOC public infrastructures; the analysis of the centralized mobility management handover support was outlined in Section 3; the distributed mobility management support for WSN based information transmission in SHM systems is presented in Section 4; and the concluding remarks in Section 5.

2. Structural Health Monitoring for SOC Infrastructures

The SOC public infrastructures SHM includes the processes of evaluation, assessment, damage detection, and continuous monitoring of engineering structures [1]. SHM includes the accumulation of various structural health information through the integration of the structure of a network of sensors that are responsible for continuously collecting and processing sensed structural signals. The collected structural health signals require a robust signal processing and filtering technique in order to quantify the location and size of damages as well as upcoming environmental disturbances and conditions. SHM systems can trigger alarms and warnings of unexpected environmental disturbances, structural risks, as well as whenever a maintenance is required [2, 3].

An efficient and robust SHM system is an essential requirement for the success of an SOC infrastructure seamless management specifically on bridges (Figure 1). Bridges require the implementation of damage detection processing as well as a dynamic response measurement from an array of installed sensors capable of monitoring environmental disturbances, occurrence of unexpected events, as well as traffic conditions. The signals collected by these sensors are required to be filtered and processed in such a way that only critical structural health signals will be transmitted for analysis and disregard unnecessary measurements, thus, makes that transmission and analysis more efficient.

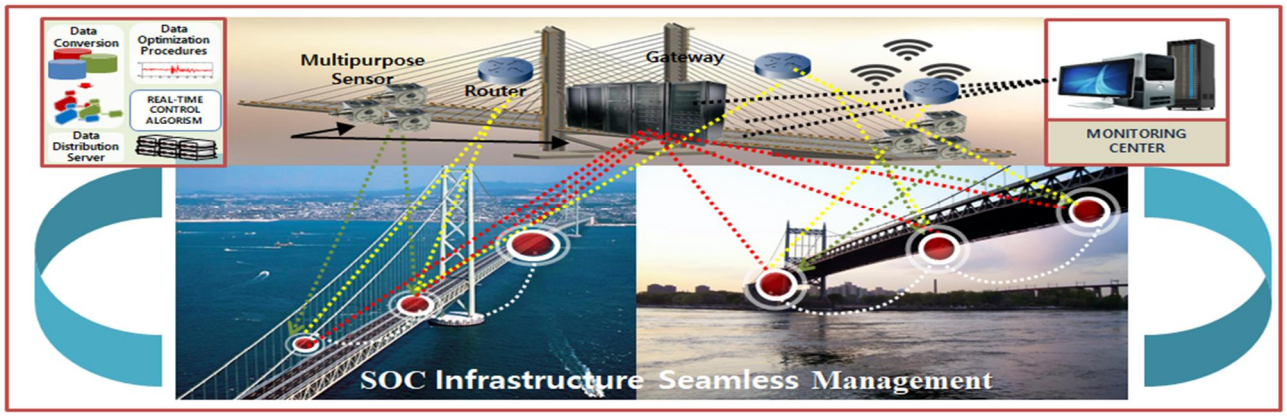


Figure 1. SOC Bridge Infrastructure Seamless Management

SHM can be applied into a variety of SOC public infrastructures, and this paper focus on the management of bridges. It is an essential part of SHM to assess the health of the structures in order to implement various measures and to ensure the safety of the public. Some of the examples of SOC public infrastructure damages caused by disasters are shown in Figure 2. The health assessment of SOC public infrastructures require the acquisition of the following information:

- detection of the occurrence of damage(s) on the SOC public infrastructure;
- damage location;
- identification of the types of damage(s);
- and quantification of the severity of the damage(s).

Figure 2. Examples of SOC Infrastructure Damages Caused by Disasters

In addition, employing signal processing, signal filtering, and statistical classification is necessary in order to convert measured sensor signals on the infrastructural health status into damage information for assessment. Thus signal monitoring processes are required in order to interpret the measured sensor signals for analysis and assessment of damages and which is essential to the prevention of untoward accidents which could lead to injuries for the public. Some examples of signal monitoring management processes are shown in Figure 3.

SHM systems includes a network of sensors, data acquisition systems, data transfer and storage techniques,

structural data management, and structural data interpretation and diagnosis. An array of sensors is installed in SOC public infrastructures (i.e. bridges) which are capable of providing real-time monitoring of various environmental disturbances and conditions as well as structural health or condition changes such as stress and strain. The measured sensor data are then transmitted into gateways which in turn forwarded these measured structural data into a remote SOC infrastructure data centers.

In this paper, the issue of data transfer is focused to be addressed since an efficient transmission of structural health and environmental status can be very critical in the seamlessness of an intelligent transportation system and can support the prevention of untoward accidents.

3. Centralized Mobility Management Handover Support

The traditional wireless systems are generally based on hierarchical systems employing centralized mobility management protocols such as the standard MIPv6 [4] and Proxy Mobile Internet Protocol version 6 (PMIPv6) [5, 6]) in handling mobility support for wireless network systems. Data traffic are generally passed through a single centralized network entity which is responsible for managing and controlling the data traffic flow as well as the mobility management of the wireless devices.

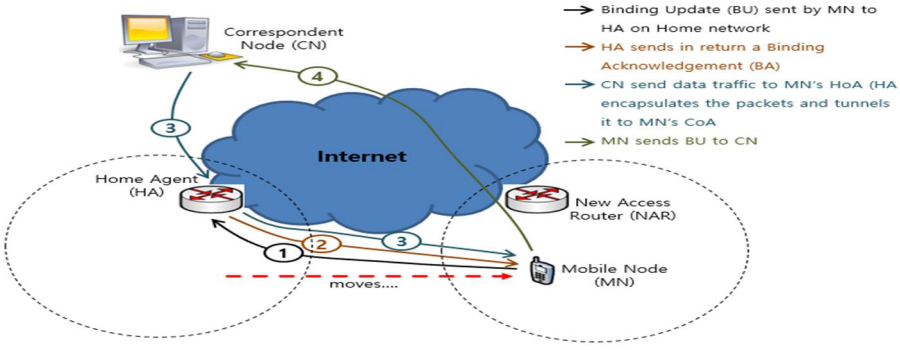
Figure 3. SHM Signal Monitoring Management

The standard MIPv6 [4] enables wireless devices to maintain its connectivity and ongoing sessions with its correspondent nodes (CNs) as it moves across the heterogeneous wireless networks. The home agent (HA) is responsible for intercepting the packets sent by the CN and deliver it directly to the MN's current location as shown in Figure 4(a). The MN is provided with two addresses, a permanent home address (HoA) allocated by its HA and a temporary care-of address (CoA) whenever it is away from its home network. The HA binds the MN's CoA with its HoA when the MN moves into another network. This is done by the HA as soon as it receives a binding update (BU) message from the MN informing its movement. The HA then sends back a binding acknowledgement (BA) message acknowledging the MN's use of the allocated CoA. This two address configuration allows MN to remain reachable for its CNs even if it is away with its home network, however, the MN continuously need to configure a new CoA every time it moves into a different network and keep on sending BU messages to the HA. This results into a higher handover latency, higher packet loss, and signaling overheads which makes MIPv6 inefficient for the implementation of SHM for SOC public infrastructures specifically if human lives will be at stake.

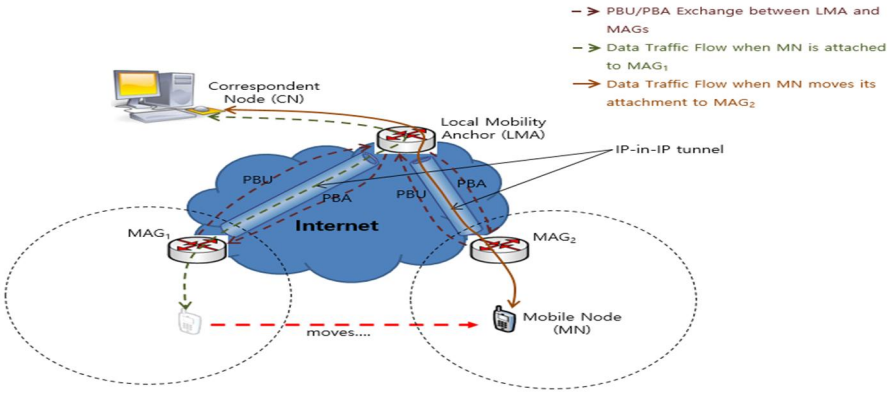
Another popular centralized system that was developed to address the inefficiencies of the standard MIPv6 is the network-based mobility management of PMIPv6 [6]. In this scheme, wireless devices are independent of the mobility related signaling as it moves from one access network to another. The mobility related

signaling were relegated to the network entities that will be responsible for the handover management of such wireless devices. As shown in Figure 4(b), binding updates were exchanged by the two network entities, the mobility access gateway (MAG), and the local mobility anchor (LMA). The MAG is responsible for implementing the mobility related signaling in lieu of the MNs currently attached into its wireless access points. The MAG is located in one of the access routers (ARs) which performs the responsibilities of detecting the MN's movements, coordinating routing states, as well as IP connectivity provisions.

On the other hand, the LMA is responsible for maintaining the collection of IP addresses of all MNs attached within the localized mobility domain (LMD). The LMA is located in the MN's home network which acts as its local HA. Whenever the MN attaches into an access point of the MAG, a bidirectional IP-in-IP tunnel will be established between the LMA and MAG. The LMA then intercepts the data traffic sent by the CN to the MN, encapsulates the intercepted data packets and tunnels them towards the MAG to where the MN is currently attached. The MAG then de-capsulate the tunneled data packets and forward them to the MN. Both the LMA in PMIPv6 and HA in MIPv6 acts as the centralized mobility anchor for the movement of MNs across the heterogeneous wireless networks as well as for the delivery of data traffic. The centralized mobility anchors serve as the central controller in the distribution of data traffic between wireless devices across the heterogeneous wireless networks. This scheme can be considered as a practical approach in managing the flow of data traffic, however, these systems can become inefficient in the case of applications requiring the transmission of real-time data traffic as well as with the increasing volume of data packets that requires immediate transmissions [7].



(a) MIPv6 Handover Process



(b) PMIPv6 Handover Process

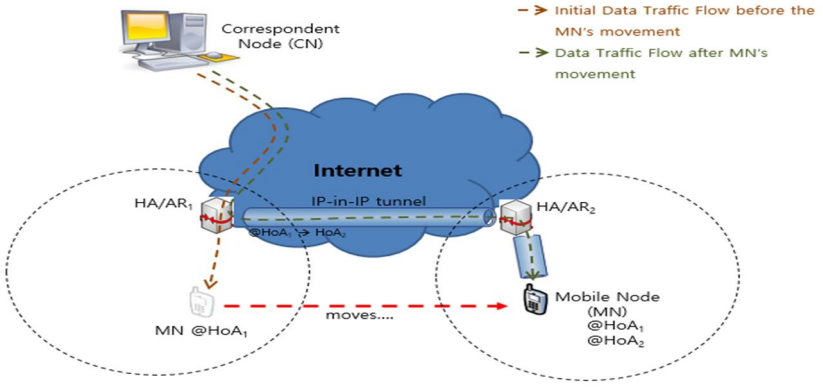
Figure 4. The Centralized Mobility Management Handover Support

Moreover, it can have a low scalability in the sense that the centralized mobility anchors are required to provide processing and routing capabilities for the data traffic of MNs. Data traffic are always navigated through the centralized mobility anchors (LMA, HA) which are located in the MN's home network resulting into a suboptimal routing. Longer paths need to be traversed by the data traffic since they need to pass through the MN's home network before such packets can be forwarded into its current location leading to unnecessary delays, higher packet loss rate and consumption of network resources. In addition, reliability and security can be greatly affected with the single point of failure for the centralized mobility anchors. Signaling overhead for centralized mobility management systems remains to be an issue since MNs and the network entities are required to exchange a number of mobility management signaling to enable the handovers between wireless access networks across the integrated heterogeneous wireless networks. Thus, as the volume of data traffic increases and the need for immediate transmission of real-time data traffic, the centralized mobility management architectures are expected to meet with performance and scalability issues. This issues encouraged the evolution of a new architectural paradigm of distributed mobility management (DMM) in order to support the handover of connectivity between wireless access networks. DMM enables the mobility anchors to be allocated at the edge of the access networks bringing them closer to the MNs. In these architectures, the MNs can transfer its point of attachment between the mobility anchors which are responsible for the distribution and control of data traffic.

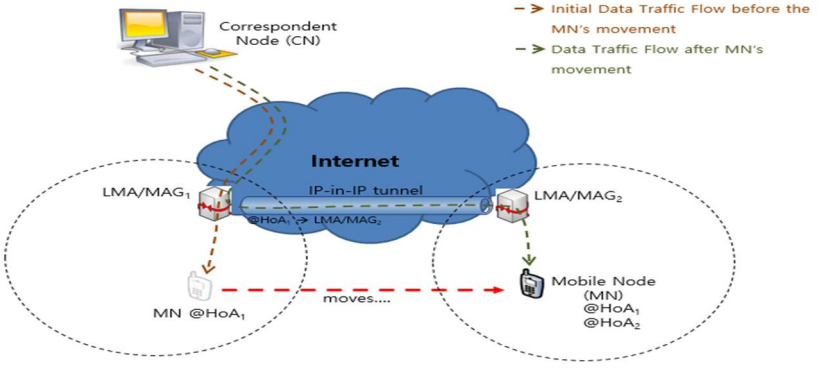
4. DMM for Information Transmission System

The standardization of distributed mobility management (DMM) has been worked out by the Internet Engineering Task Force (IETF) working group to address the issues raised in the centralized mobility management architectures. DMM has been implemented in a variety of ways: First, the client-based DMM architecture deploys multiple HAs at the edge of the access networks to serve as the mobile anchors as depicted in Figure 5(a). The MN is allocated with multiple IP addresses that binds with the locally anchored address. These multiple addresses serves as the MN's CoA whenever it changes its point of attachment [8]. The bidirectional IP-in-IP tunnels between the MN and each one of the anchoring home agents guarantee the session continuity whenever it moves from one network to the other. Initially, data traffic is traversing through the first mobility anchor (HA/AR_1) where the MN is initially attached. A new local address (HoA_2) will be allocated to the MN whenever it changes its point of attachment. This new local address serves as the CoA in the standard MIPv6 allowing MN to maintain its reachability. Whenever the CN transmits data packets to the MN, the first mobility anchor will intercept the data packets, encapsulate them and tunnels them directly to the MN's new local address via the second mobility anchor (HA/AR_2). This scheme shortens the handover latency since the mobility management has been localized and distributed among the mobility anchors which are placed at the edge of the access networks making them closer to the wireless devices. Figure 5(b) depicts the network-based DMM utilizing PMIPv6. There are two subcategories for network-based DMM: the fully distributed DMM; and partially distributed DMM. In a fully distributed DMM scheme, both the control and data plane infrastructures are managed by the mobility anchors. Each access router (AR) implements both the functions of LMA and MAG in PMIPv6 as shown in Figure 5(b). The AR will act as the LMA that anchors and routes the data traffic to the MN while serving as MAG that receives the data traffic tunneled to the MN. In a partially distributed DMM scheme, the data and control plane infrastructures are separated and the mobility anchors are only responsible for the distribution of data plane infrastructures. The control plane infrastructure is managed by a specific mobility management entity (MME). Data traffic distribution in this scheme can be optimal since it is distributed among the mobility anchors while the control of data traffic flow is managed by a single centralized network entity which an

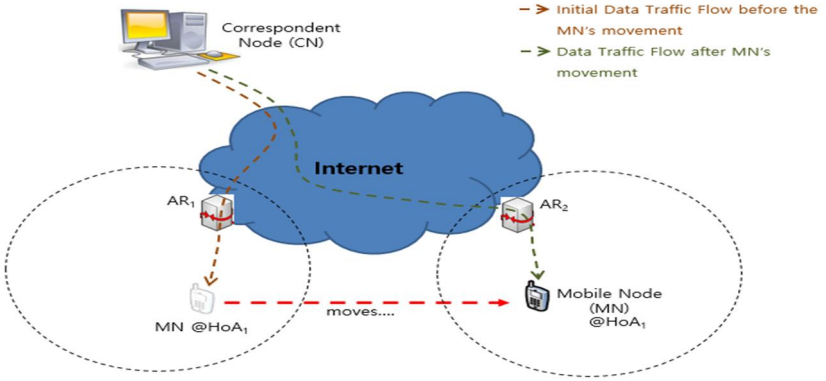
effective scheme for supporting applications requiring real-time transmissions as in SHM systems. Figure 5(b) depicts the network-based DMM utilizing PMIPv6. There are two subcategories for network-based DMM: the fully distributed DMM; and partially distributed DMM. In a fully distributed DMM scheme, both the control and data plane infrastructures are managed by the mobility anchors.



(a) Client-based DMM



(b) Network-based DMM



(c) Routing-based DMM

Figure 5. The Distributed Mobility Management Architectures

Each access router (AR) implements both the functions of LMA and MAG in PMIPv6 as shown in Figure 5(b). The AR will act as the LMA that anchors and routes the data traffic to the MN while serving as MAG that receives the data traffic tunneled to the MN. In a partially distributed DMM scheme, the data and control plane infrastructures are separated and the mobility anchors are only responsible for the distribution of data plane infrastructures. The control plane infrastructure is managed by a specific mobility management entity (MME). Data traffic distribution in this scheme can be optimal since it is distributed among the mobility anchors while the control of data traffic flow is managed by a single centralized network entity which an effective scheme for supporting applications requiring real-time transmissions as in SHM systems. Routing-based DMM scheme depicted in Figure 5(c) allows the MN to obtain an IP address as it connects into an access router. This IP address is then internally advertised by an intra-domain protocol which refers to a border gateway protocol (BGP). Whenever the node moves its connection into a new domain, the new AR finds out the IP address assigned to the MN during the authentication phase. The new AR performs a reverse lookup procedure in order to confirm that the IP address is already associated with the MN's hostname and routing updates are performed. A BGP update message is then sent by the new AR that contains the IP address of the MN to other existing routers. This DMM scheme may not be as efficient as the network-based DMM because of scalability and longer handover latency issues. This paper is focused on dealing with the handover mobility management support for information transmission in SHM systems. The network-based DMM scheme will be utilized with PMIPv6 in order to optimize the transmission of critical measured environmental disturbances, occurrence of untoward incidents, and structural health information. This system is primarily designed to prevent untoward accidents and preserve human lives for unexpected disasters that might occur. The SHM system consists of geographically installed array of smart sensors capable of measuring bridge structural health data, occurrences of untoward events, and environmental disturbances such as earthquakes, early morning fog, heavy snow or rainfall, and other natural calamities that can cause damage or failures to bridges. An efficient signal processing algorithm will be required to filter and analyze the large amount of measured and collected signals before they can be transmitted by the smart sensors into the receiving routers. In this way, only the essential and critical data signals such as important structural health data, triggering events such as vehicular accidents, scour, and earthquakes will be transmitted. This can result into a minimized network traffic disregarding the insignificant signals that can cause congestion and significant delays with the processing. The receiving routers on the other end optimizes the delivery of the received critical signals through route assessment checking on the bandwidth of every transmission path. This is done by the SHM Centralized Mobility Management (CMM) entity that acts as the centralized controller for the flow data traffic among the different mobile anchors (MAs) that resides on the access routers (ARs). The bandwidth of every transmission route can be checked using flag bits returned during the exchange of proxy binding updates (PBUs) and proxy binding acknowledgements (PBAs) between the distributed mobility management-access routers (DMM-ARs) and the CMM.

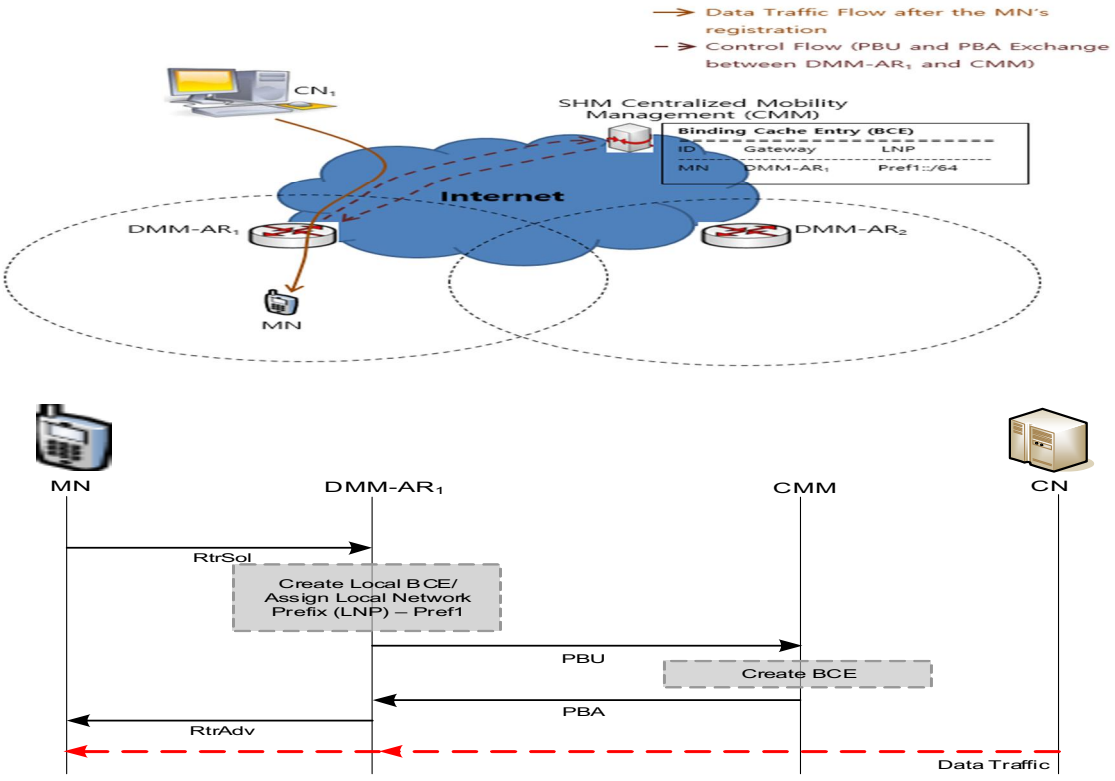
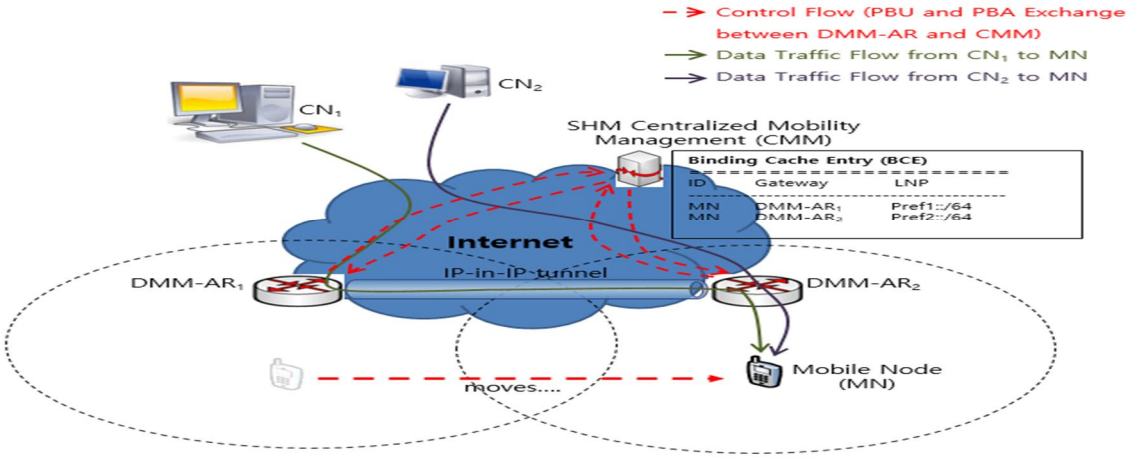


Figure 6. DMM based Information Transmission Initial Registration Process

In Figure 6, the initial registration for the DMM based mobility support for information transmission in SHM systems is depicted. The MN (e.g., smart devices on vehicles) acquires a homing address from DMM-AR$_1$ whenever it is able to attach its connection. The DMM-AR$_1$ then sends a PBU to the CMM to inform that a particular MN has attached into one of its links and CMM creates a binding cache entry (BCE) that enlists the transmission routes. The CMM returns a PBA message to the DMM-AR$_1$ acknowledging that the MN's prefix has been listed into its BCE. The CN and MN can then start to exchange data traffic. For instance, the smart device (i.e., tagged as MN on the system) on one of the vehicles can start receiving traffic information on bridges, any occurrences of naturally caused calamities, and unusual events such as vehicular accidents or heavy car traffic.



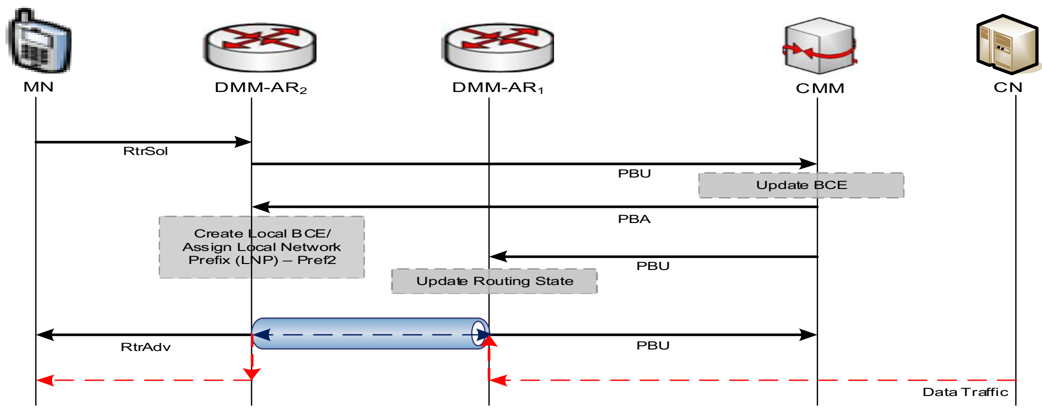


Figure 7. DMM based Information Transmission for SOC Infrastructures

Whenever the vehicle moves its point of attachment (PoA) into another router (e.g., DMM-AR_2), the new router sends a PBU message to the CMM informing that the MN will be attaching to one of its links as shown in Figure 7. The CMM updates its BCE noting that the MN moves its PoA to DMM-AR_2 sending back a PBA message. DMM-AR_2 creates its local BCE and allocates a new address for the MN. The CMM also sends a PBU message to the previous serving access router (DMM-AR_1) informing that the transmission route will be changed and a bi-directional IP-in-IP tunnel will be established between the two ARs. DMM-AR_1 sends a PBA message back to the CMM whenever the tunnel is established indicating that the session between the CN and MN will be resumed.

The CMM will be responsible on determining the optimized route for the transmission of information in SHM systems and data traffic is tunneled between the ARs. In this regard, the control plane is managed by a single centralized entity in CMM and the data traffic is distributed through the mobile anchors of the ARs. This allows the transmission distributed providing an efficient and optimal mobility management.
Upon link layer establishment, the MU sends a Router Solic-itation (RS) message to the MAAR in charge (MAAR1 in Fig. 1). The MAAR, in turn, allocates a unique LNP (pref1::MU1/64) for the MU and creates LBCE to store the MU's information, including the MU-ID and LNP. Then, the CMD creates BCE for the MU upon exchang-ing PBU/PBA messages with the MAAR and starts a new mobility session. Finally, the MAAR informs the MU of the assigned LNP through an RA message to configure an IPv6 address. The MAAR in which the MU is attached is called S-MAAR Upon link layer establishment, the MU sends a Router Solic-itation (RS) message to the MAAR in charge (MAAR1 in Fig. 1). The MAAR, in turn, allocates a unique LNP (pref1::MU1/64) for the MU and creates LBCE to store the MU's information, including the MU-ID and LNP. Then, the CMD creates BCE for the MU upon exchang-ing PBU/PBA messages with the MAAR and starts a new mobility session. Finally, the MAAR informs the MU of the assigned LNP through an RA message to configure an IPv6 address. The MAAR in which the MU is attached is called S-MAAR Upon link layer establishment, the MU sends a Router Solic-itation (RS) message to the MAAR in charge (MAAR1 in Fig. 1). The MAAR, in turn, allocates a unique LNP (pref1::MU1/64) for the MU and creates LBCE to store the MU's information, including the MU-ID and LNP. Then, the CMD creates BCE for the MU upon exchang-ing PBU/PBA messages with the MAAR and starts a new mobility session. Finally, the MAAR informs the MU of the assigned LNP through an RA message to configure an IPv6 address. The MAAR in which the MU is attached is called S-MAAR

5. Conclusion

This paper deals with the design of a DMM support for information transmission in SHM systems. The system leverages to advantages of the separation of control and data plane infrastructures of DMM architecture in order to optimize the delivery of essential and critical structural health information, occurrences of untoward accidents, environmental disturbances, and other unusual traffic events. The implementation of such system can guarantee the continuous and real-time transmission of SHM information among its different entities. A robust mobility management support of DMM and an efficient signal analysis algorithm are essentially important for the success of SHM systems that could guarantee the efficiency and safety of SOC public infrastructures.

Acknowledgement

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2018R1D1A1B07044131).

References

[1] Structural health monitoring, *https://en.wikipedia.org/wiki/Structural_health_monitoring*.

[2] J. P. Lynch, "An overview of wireless structural health monitoring for civil structures", Philosophical Transactions of the Royal Society, Vol. 365, pp. 345-372, 2007.
DOI: https://doi.org/10.1098/rsta.2006.1932.

[3] Y. Wang, J. P. Lynch, and K. H. Law, "Wireless Sensing, Actuation and Control – With Applications to Civil Structures", In: Smith I.F.C. (eds) Intelligent Computing in Engineering and Architecture, EG-ICE 2006, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, Vol. 4200, (2006).
DOI: https://doi.org/10.1007/11888598_60.

[4] C. Perkins, D. Johnson, J. Arkko, "Mobility Support in IPv6", Internet Engineering Task Force (IETF), RFC 6275, ISSN: 2070-1721, July 2011 July.

[5] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, B. Patil, "Proxy mobile IPv6", Internet Engineering Task Force (IETF), RFC 5213, August 2008.

[6] C. J. Bernardos, M. Gramaglia, L. M. Contreras, M. Calderon, I. Soto, "Network-based Localized IP mobility Management: Proxy Mobile IPv6 and Current Trends in Standardization", Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)(Special issue: Advances in Wireless Mobile and Sensor Technologies), Vol. 1, No. 2/3, pp. 16-35, 2010.

[7] H. Chan, "Requirements of Distributed Mobility Management", IETF Internet-Draft, July 2012.

[8] J. C. Zúñiga, et al., "Distributed Mobility Management: A Standards Landscape", IEEE Communications Magazine, Vol. 51, No. 3, pp. 80–7, March 2013.